



que

"יעוץ מקצועי":

נגה קרטס



שלום נחייס



מבוא לתקשורת מחשבים

מבוא
לתקשורת מחשבים

בתקליטור המצורף:

- **תמונות של ציוד תקשורת**
- **תוכנות עזר**

ועוד.....

קרא על התקליטור בנספח ד'
ובקובץ ONCD שבתקליטור

עורך מקצועי: **זהר עמיהוד**

תרגום לעברית: **גלית איטקין**



ייעוץ מקצועי: **נגה קרטס**



שלום נחייסי

עריכה לשונית ועיצוב: **שרה עמיהוד**

שמות מסחריים

שמות המוצרים והשירותים המוזכרים בספר הינם שמות מסחריים רשומים של החברות שלהם. הוצאת QUE והוצאת הוד-עמי עשו כמיטב יכולתן למסור מידע אודות השמות המסחריים המוזכרים בספר זה ולציין את שמות החברות, המוצרים והשירותים. שמות מסחריים רשומים (registered trademarks) המוזכרים בספר צוינו בהתאמה.

Windows 95/98/ME, Windows NT/2000 הינם מוצרים רשומים של חברת Microsoft.

הודעה:

ספר זה מיועד לתת מידע אודות מוצרים שונים. נעשו מאמצים רבים לגרום לכך שהספר יהיה שלם ואמין ככל שניתן, אך אין משתמעת מכך כל אחריות שהיא.
המידע ניתן "כמות שהוא" ("as is"). הוצאת QUE והוצאת הוד-עמי אינן אחראיות כלפי יחיד או ארגון עבור כל אובדן או נזק אשר ייגרם, אם ייגרם, מהמידע שבספר זה, או מהתקליטור המצורף לו.

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

- טלפון: 09-9564716
- פקס: 09-9571582
- דואר אלקטרוני: info@hod-ami.co.il
- אתר באינטרנט: www.hod-ami.co.il

מבוא
לתקשורת מחשבים

דן יורק







Introduction to Computer Networks

based on: **Networking Essentials Exam Guide**

By **Dan York**

Editor: **Z. Amihud**

Hebrew Translation: **G. Itkin**

הוצאת הוד-עמי לספרי מחשבים בע"מ
ת.ד. 6108 הרצליה 46160
טלפון: 09-9564716 פקס: 09-9571582
info@hod-ami.co.il
www.**hod-ami**.co.il

הודפס בישראל 2000

HOD-AMI Ltd.
P.O.B. 6108, Herzliya
ISRAEL, 2000

ISBN 965-361-273-5 מסת"ב

תוכן עניינים מקוצר

תוכן העניינים

פרק 2: מודל הייחוס OSI ... 43

פרק 3: רשתות מקומיות - LAN ... 53

פרק 4: החיבור הפיסי 67

פרק 5: חיבורי אלחוט 84

פרק 6: תמסורת נתונים - Data Transmission 100

פרק 9: מערכות הפעלת רשת....................................167

פרק 10: יישומי רשת..177

פרק 11: גישה מרחוק 189

פרק 12: רכיבי קישוריות / רשתות גדולות........................201

פרק 13: רשתות מרחביות (WANs)................................218

פרק 14: האינטרנט 235

פרק 17: פתרון בעיות 290

הקדמה

"המחשב הוא הרשת" התנבא מנכ"ל חברת SUN בשלהי 1998 ו...בשנת 2000 חזר על זה, אמנם במילים אחרות, מנכ"ל מיקרוסופט ביל גייטס, והכריז על Microsoft.NET. אכן נושא התקשורת הוא אחד ממפתחות הכניסה לעולם ההיי-טק. אין זה משנה אם אתה מתכוון להיות Web Master, Web Designer, Software Engineer, Database Engineer, System Engineer, System Administrator, Web Programmer וכמובן Network Design Engineer או משרה אחרת בעולם ההיי-טק, אתה חייב להבין בתקשורת. אתה חייב לדעת "מי נגד מי?" ולקשר "מה מתחבר עם מה? ואיך?".

על מה הספר

הספר "מבוא לתקשורת מחשבים" ילמד אותך מהתחלה את יסודות התקשורת. כל מה שתלמד מעבר לספר זה יהיה קשור, בצורה זו או אחרת, לידע שרכשת בעולם התקשורת בעזרת ספר זה.

יכולתך להבין טכנולוגיות חדשות, כגון: WAP, xDSL, SMS, IM מושתת על הבנתך ביסודות התקשורת - אותם תלמד בעזרת ספר זה.

על מה זה לא

זה לא ספר תקשורת למערכות Microsoft Windows כמו שזה לא ספר למערכת Novell או UNIX. מרבית הדוגמאות הקשורות למערכת הפעלה מקורן במערכת הפעלה מסוג Windows רק בגלל הנוחות שבעניין.

זה לא ספר לציוד תקשורת של Intel כמו שזה לא ספר לציוד תקשורת של Cisco, SMC או כל חברה אחרת.

כיצד ללמוד בעזרת ספר זה

הפרקים בספר זה מיועדים לקריאה לפי סדר הופעתם. כל פרק מסתמך על החומר הנלמד בפרקים הקודמים.

כיצד ספר זה מאורגן

הספר מחולק ל-17 פרקים, כל אחד מהם מתמקד בנושא מסוים המהווה חלק חשוב בתמונה הכוללת.

- **פרק 1**, "הקדמה לרשתות", הוא סקירה כללית של רשתות מחשבים. נסקרים המונחים הבסיסיים, סוגי הרשתות השונים, והרכיבים המרכיבים רשת. פרק זה מציג גם את עקרונות רישות המחשבים שבהם נעסוק בהמשך הספר.
- **פרק 2**, "מודל הייחוס OSI", מציג מודל תיאורטי של אופן פעולת רשת. יוצג רעיון הרישות בשכבות וכל שכבה של מודל ייחוס OSI תידון בפירוט. רשתות מציאותיות יושוו למודל התיאורטי.
- **פרק 3**, "רשתות מקומיות - LAN", מספק מידע קריטי לתכנון רשת. יידונו רשתות אפיק, כוכב וטבעת, ותלמד איזו רשת מתאימה למצבים שונים.
- **פרק 4**, "החיבור הפיסי", מתחיל בשכבה הפיסית של מודל OSI ומציג את הרכיבים הפיסיים הדרושים ליצירת רשת מחשבים. יוערכו סוגי תווך שונים, ויישקלו היתרונות והחסרונות שלהם.
- **פרק 5**, "חיבורי אלחוט", דן בחלופות אלחוטיות לחיבורי הכבלים המתוארים בפרק 4.
- **פרק 6**, "תמסורת נתונים - Data Transmission", מתבונן בפונקציות בשכבת קישור הנתונים של מודל OSI, ובמיוחד בדרך שבה הנתונים נארזים לחבילות לצורך העברה על פני התווך הפיסי של הרשת. פרק זה גם סוקר את השיטות השונות שבהן רשתות משתמשות כדי לקבוע איזה מחשב יכול להעביר נתונים אל הרשת.
- **פרק 7**, "ארכיטקטורת רשת (שיטות גישור)", משלב את המידע הנידון בפרקים הראשונים. חמישה מבנים שונים של רשתות יוצגו ויוגדרו בהתאם לטופולוגיה שלהם, תווך פיסי, ושיטת גישת הנתונים לרשת. תלמד את היתרונות והחסרונות של חמש ארכיטקטורות הרשת ומתי כל ארכיטקטורה מתאימה.
- **פרק 8**, "פרוטוקולי רשת", מציג את הפרוטוקולים השונים המהווים את השכבות העליונות של מודל OSI. תשומת לב מיוחדת תוקדש ל-TCP/IP, IPX/SPX ו-NetBEUI, מכיון שאלה הם שלושת הפרוטוקולים הנפוצים ביותר בסביבות מיקרוסופט.
- **פרק 9**, "מערכות הפעלת רשת", דן בתפקיד מערכות הפעלה במסגרת סביבה מרושתת. היתרונות של מערכות הפעלה שונות יידונו עם התמקדות מיוחדת ב-Windows NT ו-Windows 2000.
- **פרק 10**, "יישומי רשת", מתמקד בסוגי היישומים הנמצאים בסביבת רשת אופיינית. בנוסף יישקלו הגורמים הקשורים במימוש יישומי רשת בסביבה אמיתית.

* **פרק 11,** "גישה מרחוק", מספק הבנה של הנושאים סביב מתן אפשרות למשתמשים לגשת לרשת מרחוק. יידונו הטכנולוגיות הקשורות ונושאי האבטחה.
* **פרק 12,** "רכיבי קישוריות / רשתות גדולות", מציג שיטות שונות להרחבת הרשת עם גידול הארגון. התקנים כגון גשרים, נתבים ושערים יתוארו ויושוו זה לזה.
* **פרק 13,** "רשתות מרחביות (WANs)", מסביר את האפשרויות העומדות בפניך בעת קישור מספר רשתות על פני אזורים גיאוגרפיים נרחבים. תיכנס לעולם של ראשי התיבות בטלקומוניקציה ותלמד את המשמעויות שלהם.
* **פרק 14,** "האינטרנט", מתאר את אופן הפעולה של האינטרנט ואילו שירותים זמינים עם חיבור הרשת שלך לאינטרנט.
* **פרק 15,** "ניהול רשת", דן בנושאים ובטכניקות הקשורים לניהול למעשה של רשת. תלמד כיצד ליצור משתמשים ולהתייחס לנושאי אבטחה בסביבות Windows NT ו-Windows 2000.
* **פרק 16,** "מניעת תקלות ברשת", מתמקד בשיטות שבהן ניתן להשתמש למניעה (או צמצום) של הבעיות ברשת. פרק זה יסביר טכנולוגיות אפשריות, את היתרונות שלהן, וכיצד ניתן לממש אותן.
* **פרק 17,** "פתרון בעיות", מציג את המשאבים והטכנולוגיה הזמינים לסייע לך בפתרון בעיות ברשת.

לסיום, הנספחים בספר זה מספקים משאבים ומידע נוספים העשויים להועיל בעת הלימוד:

* **נספח א',** "טבלאות סיכום".
* **נספח ב',** "מילון מונחים", מספק הגדרות של מונחים שעליך להכיר כאיש מקצוע בתחום הרשתות.
* **נספח ג',** "משאבים מומלצים", מציג רשימה של משאבים נוספים (ספרים, אתרים באינטרנט) לקריאה בנושא תקשורת נתונים.
* **נספח ד',** "שימוש בתקליטור", מספק מידע בסיסי אודות ההתקנה והשימוש בתקליטור המצורף לספר זה.

מה בתקליטור

בתיקיה **Books\59304** צירפנו קטלוג של חברת טלדור, ישראל. חברת טלדור מתמחה בייצור כבלים לתקשורת מחשבים, מובילה בתכנון ובייצור כבלים להעברת נפחי מידע גבוהים במיוחד. המפעל נמצא בקיבוץ עין דור.

הקטלוג מכיל פרטים של אלפי הכבלים, כולל תמונות, מפרט טכני, תרשימים ופרטים נוספים.

להתקנת הקטלוג יש להפעיל את הקובץ Setup.exe

אתם מוזמנים לבקר באתר של חברת טלדור בכתובת:

www.teldor.com

בנוסף תמצא בתקליטור:

- קטלוג HTML של הוצאת הוד-עמי ותוכניות שירות שונות.
- תוכנת גלישה Microsoft Internet Explorer 5 הגירסה העברית.
- עשרות תוכנות עזר מובחרות שיחסכו לך זמן הורדה יקר מהאינטרנט.

מידע נוסף בנספח ד' ובאתר האינטרנט

אתה מוזמן לבקר באתר האינטרנט של **הוצאת הוד-עמי**, בכתובת

http://www.hod-ami.co.il

תכונות מיוחדות של ספר זה

בספר זה נעשה שימוש בתכונות הבאות.

הערות

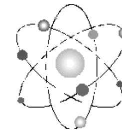
הערות מציגות מידע נוסף מעניין ומועיל. מידע זה משפר את הבנתך בתחום הרישות, אולם תוכל לדלג על הערות מבלי להסתכן באובדן מידע חיוני. הערות נראות כך :



הערה: את מרבית היישומים לא ניתן להתקין על שרת קבצים כך שישמשו את כל משתמשי הרשת. במקרים רבים יש לרכוש "גרסת רשת", או לפחות "רשיונות לקוחות" עבור כל משתמש שישתמש בתוכנה.

On the Web

הערות On the Web מציגות מידע נוסף מעניין או מועיל שאינו בהכרח חיוני לדיון והנמצא ב- Web. הערות על ה-Web נראות כך :



על ה- Web

ארגון התקינה IEEE מפרסם תקנים באתר http://www.ieee.org.

טיפים

טיפים מציגים עצה קצרה בנושא תהליכים, רעיונות קצרים, או כאלה שיש נטייה לא לשים לב אליהם. אלה כוללים קיצורי דרך החוסכים זמן, או דרכים לזכור מידע שיסייעו לך בעולם האמיתי. טיפ נראה כך :



טיפ: שכבת התצוגה מכינה את **הנתונים** להיות **מוצגים** לרשת (אם בדרכם החוצה) או ליישום (אם בדרכם פנימה).

רעיון מפתח

רעיון מפתח מצביע על אותם רעיונות שהם חיוניים להצלחתך כאיש מקצוע בתחום הרשתות. שים לב אליהם, וודא שאתה מבין את כל רעיונות המפתח.



רעיון מפתח

כדי שתתרחש תקשורת בין שני מחשבים על רשת Ethernet, על שניהם להשתמש בסוג מסגרת זהה.

בנוסף לתכונות מיוחדות אלו, נעשה שימוש במספר מוסכמות בספר זה כדי שיהיה קל יותר לקריאה ולהבנה. מוסכמות אלו כוללות שילובי מקשי קיצור, פקודות תפריט, והדגשות סוג אות (typeface).

צירופי מקשי קיצור

בספר זה, צירופי מקשי קיצור מחוברים בסימן חיבור (+). לדוגמה, Ctrl+V פירושו: הקש על מקש Ctrl ובעודו לחוץ, הקש גם על V.

פקודות תפריט

במלל, הוראות לבחירת פקודות מתפריט מוצגות בתצורה הבאה: בחר File, New.

פירוש דוגמה זו הוא פתח את התפריט File ובחר בפקודה New, שבמקרה זה פותחת קובץ חדש.

מערכות הפעלה

בכל מקום בספר בו מופיעה התייחסות למערכת ההפעלה Windows 95 יש לראות זאת גם כהתייחסות למערכת ההפעלה Windows 98 או Windows ME. בדומה, התייחסות למערכת ההפעלה Windows NT Workstation יכולה להיחשב כהתייחסות ל-Windows 2000 Professional, אבל ברמת ה-Server יש לשים לב. לא כל מה שנכון עבור Windows NT Server נכון וישים עבור Windows 2000 Server. מעבר לכך, למערכת ההפעלה Windows 2000 Server יש הרבה יותר שירותים מקודמתה.



הקדמה לרשתות

פרק זה מציג בפניך את היסודות של **רישות מחשבים** (computer networking), וכולל:

- סיבות לרישות,
- מונחים שיש להכיר בתחום הרישות,
- סוגי הרשתות השונות,
- התפקידים השונים של שרתים ברשת,
- ביצוע החיבור הפיסי.

למה להשתמש ברשתות?

כיצד **רשתות מחשבים** (computer networks) מפשטות את העבודה? כיצד יכול העסק שלך ליהנות מרישות מחשבים? למה להיכנס לרישות מחשבים? נשקול כל אחד מהמצבים הבאים:

- אתה פועל במשרד קטן שבו מחשבים שונים אינם מחוברים למדפסת. בכל פעם שאתה רוצה להדפיס, עליך לשמור את המידע על דיסקט ולהעבירו פיסית למחשב המחובר למדפסת. במשך יום עבודה מצב זה יכול לחזור על עצמו מספר פעמים, ובכל פעם אתה מפריע לזרימת העבודה שלך ושל עמיתיך לעבודה.
- בחברת הייעוץ שבה אתה עובד, מספר אנשים צריכים לעבוד על אותה קבוצת מסמכים. אתה מבלה זמן רב בהעתקת קבצים לדיסקטים ואז מעביר (מעתיק) אותם למחשבים של שאר האנשים, כדי שיוכלו להשתמש בהם. עם הזמן תגלה שקשה יותר לעקוב אחר המיקום של הגירסה המעודכנת ביותר של כל מסמך.

כתוצאה מכך, אנשים עלולים לעבוד על גרסאות שונות שאינן תואמות, ונוצרות בעיות רבות בניסיון לתאם דברים.

* לחברה שלך יש מספר משרדים המפוזרים באזור גיאוגרפי גדול. בגלל הצורך בתקשורת בין-משרדית, כל משרד מקדיש זמן, עבודה וכסף ביצירת מידע על מחשבים, ואחר כך - צריך לשלוח פקסים בין משרדים או להכין מסמכים מודפסים למשלוח עם שליח או בדואר מהיר.

* עובדים בארגון המכירות שלך משתמשים רבות במכשיר הפקס ומבלים חלק ניכר מיום העבודה שלהם בהמתנה לזמינות המכשיר. מכשיר הפקס הופך לצוואר בקבוק בדרך לקבלת נתוני מכירות ומידע נוסף. יש לך מודם-פקס על אחד המחשבים, אולם רק אדם אחד יכול להשתמש בו.

בכל המקרים האלה רשתות מחשבים יכולות לפתור בעיות עסקים אמיתיות ולהגביר את היעילות והתפוקה של הארגון. ספר זה דן בפתרון בעיות אלו ובעיות דומות רבות הפוקדות את העולם הממוחשב. בין אם התשובה היא שיתוף מדפסות ומכשירי מודם-פקס, אחסון קבצים מרכזי, או אפשרות תקשורת פשוטה ברחבי הארגון, רישות מחשבים הוא הכלי למימוש פתרונות אלה.

מהרשת המקומית במשרד אל רשת האינטרנט העולמית, מחשבים מקיפים אותנו וממלאים תפקיד קריטי בפעילות היומיומית של ארגונים מכל הגדלים. ספר זה יסייע לך להבין כיצד רשתות אלו פועלות, וכיצד תוכל להשתמש בהן כדי לסייע לארגון שלך.

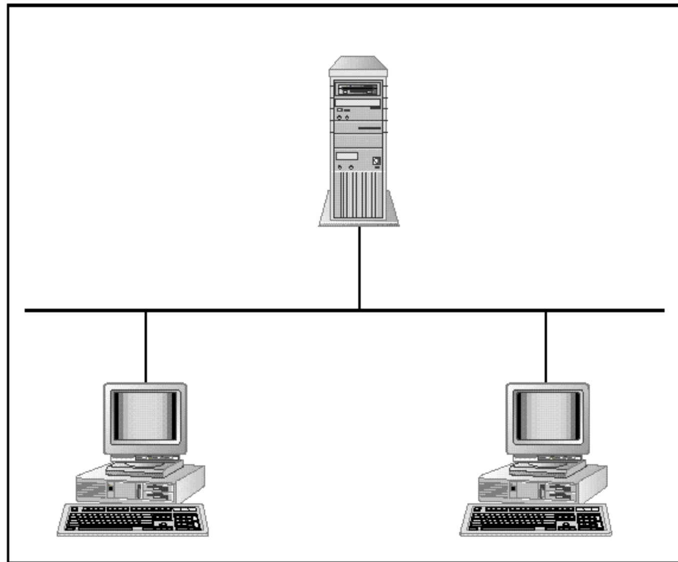
מונחי רישות

לפני שנמשיך, עלינו לעצור ולדון בשפה המשמשת לתיאור רשתות. רשתות תקשורת מחשבים יצרו רשימה כמעט אינסופית של מונחים חדשים, וחלק ניכר מהקושי בלימוד רשתות הוא הבנת המונחים האלה.

לקוחות, שרתים ושוויונים

כל מחשב ברשת משמש כ**לקוח** (client) או **שרת** (server). מחשב שהוא **שרת** "משתף" משאבים ברשת. מחשב שהוא **לקוח**, משתמש במשאבים אלה. בכל אינטראקציה בין מחשבים ברשת, אחד המחשבים ישמש כלקוח והאחר ישמש כשרת. תצורת רשת אופיינית ניתן לראות בתרשים 1.1.

בעוד שסוגים אחדים של רשתות מגבילים מחשבים לתיפקוד כלקוח או כשרת, סוגים אחרים של רשתות מאפשרים למחשב לשמש הן כלקוח והן כשרת. כך יכולים מחשבים אלה להשתמש במשאבי רשת, וגם לשתף מחשבים אחרים במשאבים שלהם. מחשבים הפועלים כך נקראים **שוויונים** (peers). מערכות הפעלה כגון Windows 9x, Windows NT ו-Windows 2000 תומכות **ברשת שוויונית** (peer-to-peer network).



תרשים 1.1: *ברשת מחשבים השרתים משתפים משאבים ולקוחות משתמשים במשאבים המשותפים*

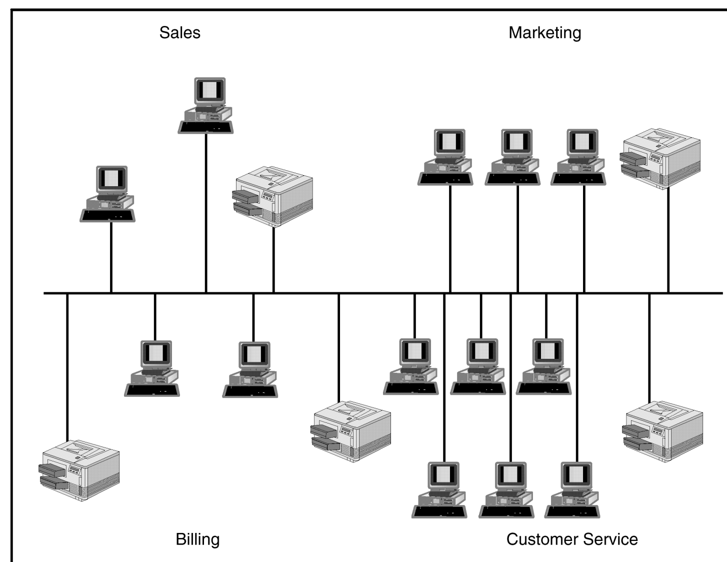
תווך רשת, רשתות תקשורת מקומית ורשתות מרחביות

מחשבים מחוברים באמצעות **תווך רשת** (network media). ברוב הרשתות, אלה הם כבלי נחושת המחברים בין המערכות. אולם, תווך הרשת יכול גם להיות סיבים אופטיים, או טכנולוגיה אלחוטית כגון מיקרוגל, או אינפרא-אדום. בכל המקרים, החיבורים הפיסיים נקראים **תווך** (media). מחשב מחובר לתווך באמצעות **כרטיס ממשק רשת - NIC** (Network Interface Card), הנקרא גם **מתאם רשת** (network adapter).

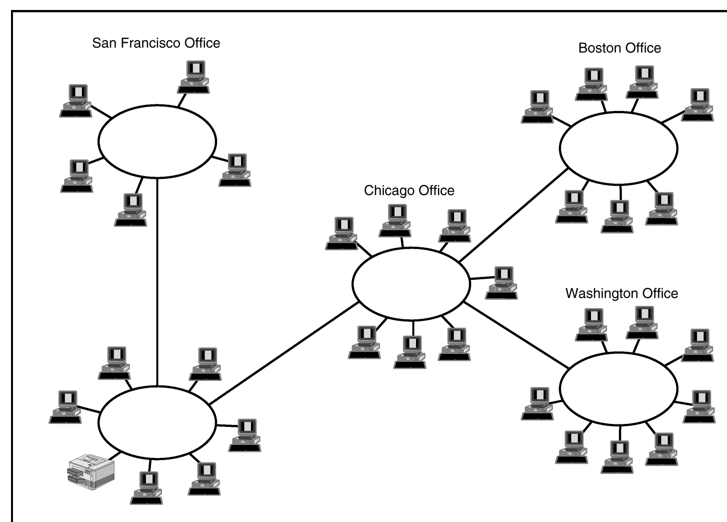
כאשר מספר מחשבים מחוברים יחד באזור מצומצם יחסית, כגון בניין משרדים, הרשת נקראת ***רשת תקשורת מקומית - LAN*** (Local Area Network). כפי שניתן לראות בתרשים 1.2, רשת מקומית יכולה לכלול מחשבים רבים ושונים, בנוסף למשאבים אחרים, כמו מדפסות. מגבלות כבלים פיסיים מגבילות במקרים רבים רשתות מקומיות למרחקים קצרים מ-150 עד 180 מטר (500-600 feet).

עם הגידול ברשתות מקומיות אלו וחיבור של שתי רשתות או יותר לרשת מקיפה אחת, לעיתים על פני מרחק גיאוגרפי גדול, אנו משיגים ***רשת תקשורת מרחבית - WAN*** (Wide Area Network).

תרשים 1.3 מציג רשת מרחבית המקשרת חמש רשתות אזוריות.



תרשים 1.2: *רשת מקומית מקשרת מחשבים באזור קטן*



תרשים 1.3: *רשת מרחבית מקשרת רשתות מקומיות נפרדות, בדרך כלל על פני מרחק גיאוגרפי גדול*

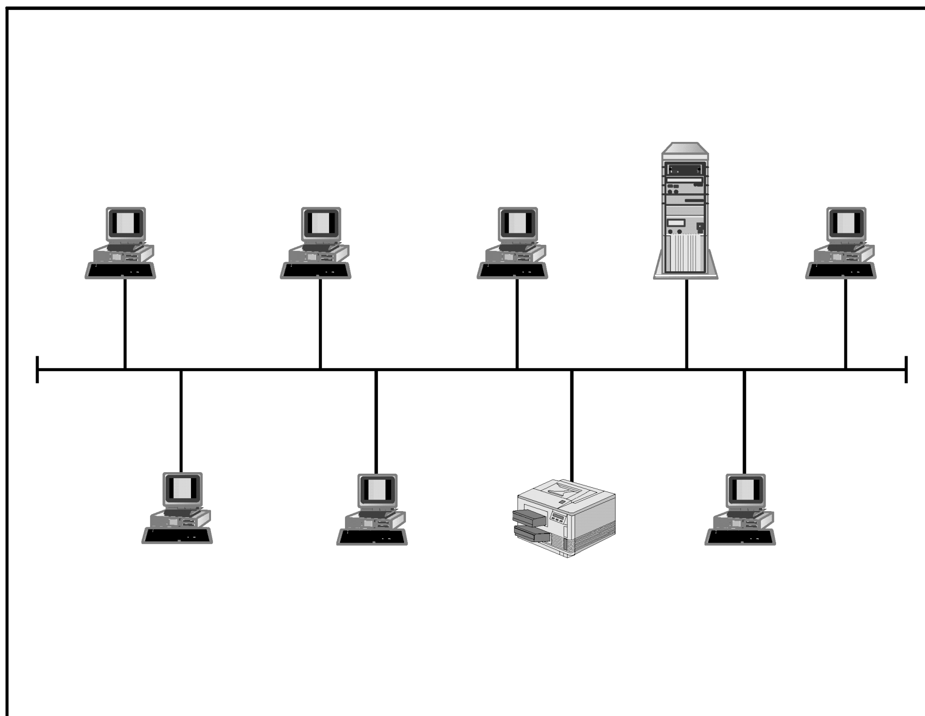


הערה: המונח **רשת תקשורת מטרופוליטנית - MAN** (Metropolitan Area Network), מתאר למעשה רשת המשתמשת בטכנולוגיות WAN לקישור רשתות LAN באזור גיאוגרפי מוגבל, כמו עיר. לדוגמה, חברה כלכלית גדולה עשויה לקשר מספר רשתות מקומיות בחלקים שונים של העיר ליצירת רשת מטרופוליטנית. רשת זו תקושר לרשתות בערים אחרות ליצירת רשת מרחבית. כלומר, המונח MAN מתאר שימוש, ולאו דווקא טכנולוגיה, או תפישה.

טופולוגיה

אם תשרטט תרשים של אופן החיבור הפיסי של המחשבים שלך, התרשים ייצג את **טופולוגיית הרשת** (network topology). קיימים שלושה סוגים עיקריים של טופולוגיית רשתות. מונחים אלה יתוארו בפירוט בהמשך, והם מובאים כאן בקיצור כדי לסייע ביצירת תמונה ברורה של רישות.

ב**רשת אפיק** (bus network), כפי שמוצג בתרשים 1.4, כל המחשבים מחוברים בשורה. הודעות מועברות בין מחשבים לאורך **אפיק שידרה** (backbone) יחיד המקשר ביניהם. בכל קצה של אפיק שידרה זה נמצא **נגד סיום** (terminator) לעצירת אות הרשת.



תרשים 1.4: *רשת אפיק מקשרת את כל המחשבים בקו אחד*

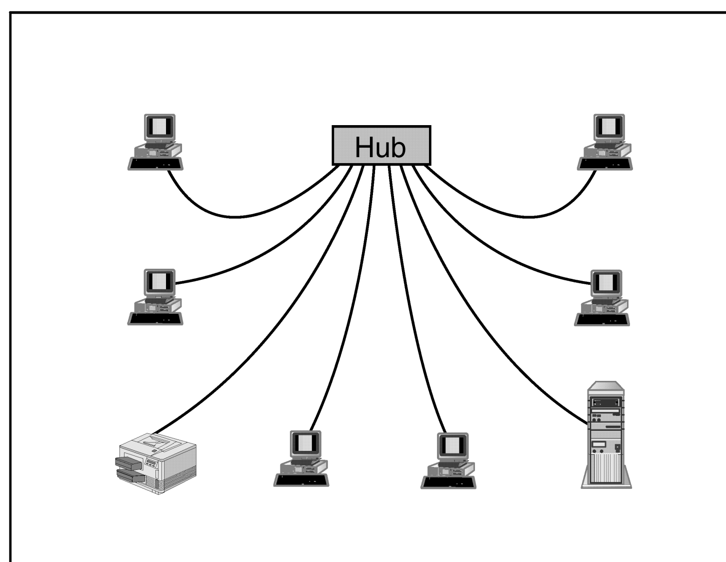
כפי שמוצג בתרשים 1.5, **רשת כוכב** (star network) משתמשת ב**רַכֶּזֶת** (hub) לקישור כל המחשבים. הרכזת משמשת כאתר איסוף וחלוקה מרכזי לכל תעבורת הרשת.

לסיום, טופולוגיית **טבעת** (ring) מקשרת את כל המחשבים בטבעת יחידה. כפי שמוצג בתרשים 1.6, המידע מועבר בטבעת רציפה.

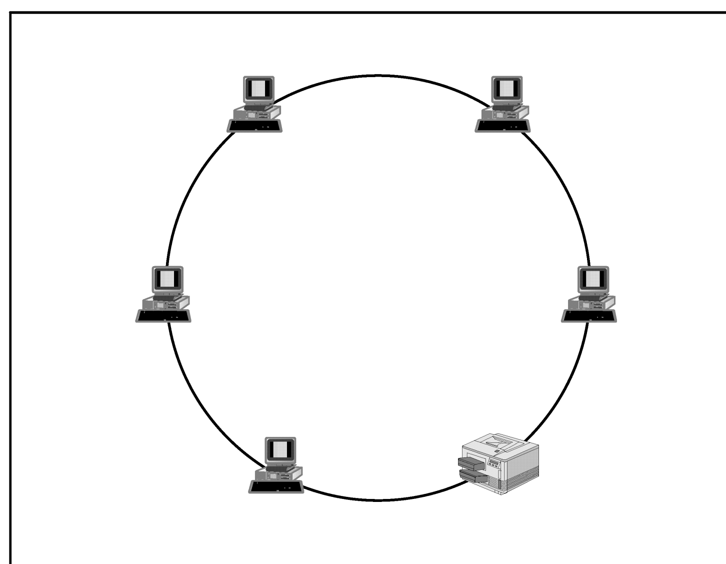
המונח **ארכיטקטורת רשת** (network architecture) מתייחס בדרך כלל לשיטה שבה **מנות** נתונים (packets) מועברות על פני **תווך הרשת** (network media). לדוגמה, כאשר מדובר ברשת **איתרנט** (Ethernet) או **טבעת אסימון** (Token-Ring), זהו תיאור של **ארכיטקטורת הרשת**. לעיתים משתמשים במונח **ארכיטקטורת רשת** לתיאור המבנה הכולל של הרשת, כולל הטופולוגיה.



הערה: המונח **תווך הרשת (network media) מתאר את סוג החיבור בין מחשבים בו יעברו מנות הנתונים. תווך זה יכול להיות כבל, תשדורת אלחוטית, תקשורת מיקרוגל, תקשורת לווין או כל סוג תקשורת אחר.**



תרשים 1.5: *בטופולוגיית כוכב, רכזת מקשרת את כל המחשבים זה לזה*



תרשים 1.6: *טופולוגיית טבעת מקשרת בין כל המחשבים במעגל*

פרוטוקולי רשת

לאחר החיבור ביניהם, צריכים המחשבים לדעת כיצד לתקשר זה עם זה. במונחים של תקשורת בין בני אדם, אם אני אתקשר אליך בטלפון ואדבר בעברית בלבד ואתה דובר צרפתית בלבד, הסיכויים שלנו לניהול שיחה בעלת משמעות הם, למעשה, אפסיים. באופן דומה, שני מחשבים חייבים להשתמש באותה שפה כדי לתקשר. השפה שבה הם משתמשים נקראת **פרוטוקול רשת** (network protocol), אשר מתוארת בדרך כלל בראשי תיבות כגון : TCP/IP, IPX, DLC, ואחרים.

תוכנת רשת

בנוסף לפרוטוקול, דרושה למחשבים **מערכת הפעלת רשת** (network operating system) המבקרת על הגישה למשאבי הרשת. מערכות הפעלת הרשת הנפוצות ביותר הן Windows NT/2000 ו- Novell NetWare.

מעל מערכת ההפעלה נמצאים **יישומי הרשת** המתקשרים על פני הרשת. יישומים או תוכניות אלה יכולים להיות תוכניות **דואר אלקטרוני (e-mail)**, **מנהל הקבצים (File Manager)**, מערכות לניהול הדפסה ועוד.

נשלב כל זאת יחד ונוכל להגדיר זאת כך : **יישומי הרשת** שלך רצים על **מערכת הפעלת רשת** המשתמשת ב**פרוטוקול** כדי לתקשר על פני **תווך** הרשת עם מחשבים אחרים ב**רשת המקומית**. רשת מקומית זו בנויה **בטופולוגיה** מסוימת ומשתמשת ב**ארכיטקטורת רשת** להעברת **מנות** נתונים בין מחשבים.

הבנת? אל תדאג - עד לסוף הלימוד בספר זה, תבין משפט זה היטב!

סוגי רשתות

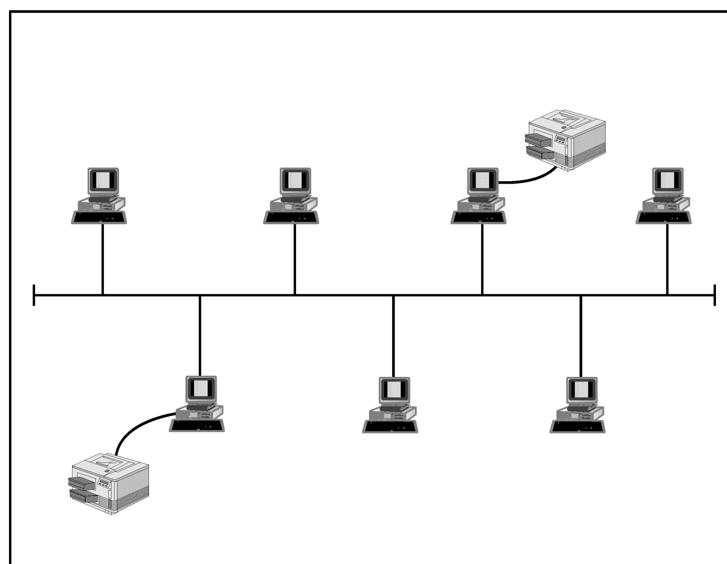
ניתן לחלק רשתות מחשבים לשני סוגים עיקריים :

- ✯ רשתות **שוויוניות** (peer-to-peer),
- ✯ רשתות **מבוססות שרת** (server based).

למרות שרשתות מבוססות שרת הן התקן במרבית הארגונים כיום ויהוו את המוקד לחלק ניכר מספר זה, יש להבין את שני סוגי הרשתות.

רשתות שוויוניות

ברשתות שוויוניות (peer-to-peer), כמו זו המתוארת בתרשים 1.7, כל מחשב יכול לשמש הן כשרת (משתף משאבים) והן כלקוח (משתמש במשאבים). אין ברשת כזו בקרה מרכזית על משאבים, כגון קבצים או מדפסות. משתמשים שונים משתפים משאבים מתי ועם מי שהם רוצים. כל המחשבים שווים בכך שאין מחשב בעל עדיפות גבוהה יותר לשימוש במשאבים ברשת.



תרשים 1.7: *ברשת שוויונית, כל מחשב יכול לשתף משאבים וגם להשתמש במשאבים שנמצאים במחשבים אחרים*

הגישה ברשת שוויונית מבוקרת על ידי המשתמש המשתף את המשאב. המשתמש יכול לאפשר גישה מלאה לכל משתמשי הרשת האחרים, לאשר גישה מוגבלת, או לדרוש סיסמה לפני הרשאה להשתמש במשאב השייך לו.

מסיבה זו, אבטחה היא עניין מרכזי ברשתות שוויוניות. כל המחשבים מקובצים ל**קבוצות עבודה** (workgroups), אך אין בקרות אבטחה על כלל הרשת. אם אתה יודע את הסיסמה המאפשרת גישה למשאב כלשהו, תוכל לגשת אליו. החיסרון הוא, שהצורך בסיסמה נפרדת לכל אחד מהמשאבים המשותפים עלול לגרום למשתמשים לטבוע בים של סיסמאות שונות שעליהם לזכור.

נושא מרכזי נוסף ברשתות שוויוניות הוא בכך שמחשבים ברשתות מסוג זה בדרך כלל אינם עוברים אופטימיזציה לביצועי רשת. המחשבים מיועדים בעיקר ליישומים משרדיים, אולם יש להם גם יכולת לשתף משאבים. פירוש הדבר הוא שכאשר משתמש אחר מתחיל להשתמש במשאבים משותפים הנמצאים על המחשב שלך, או קשורים למחשב שלך, תרגיש ירידה בביצועי המערכת שלך. אם אתה משתף את המדפסת שלך עם הרשת, המערכת (המחשב) שלך תואט בכל פעם שמישהו אחר ידפיס בה.

ארגון הנתונים בקבצים או במסדי נתונים עלול אף הוא להיות נושא בעייתי ברשת שוויונית. אם הכול יכולים לשתף נתונים, איך עוקבים היכן הם נמצאים? לדוגמה, במשרד קטן, משתמש אחד עשוי לשתף תיקיה המכילה קבצים של גיליון אלקטרוני. משתמש אחר עשוי לשתף תיקיה המכילה מסמכים כלכליים והודעות לעיתונות. אחר עשוי לשתף את מידע המכירות המעודכן. אם אתה מחפש מסמך מסוים, ייתכן ותצטרך לחפש במספר מחשבים לפני שתמצא את הנתונים הדרושים לך. ללא אזור אחסון מרכזי, מציאת מידע עלולה להיות משימה מורכבת.

חסך זה באזור אחסון מרכזי מקשה גם על הגנת המידע באמצעות גיבוי. אם הנתונים מאוחסנים במחשבים שונים, יש לגבות כל אחד מהם בנפרד. אין דרך פשוטה לגיבוי כל הנתונים.

עם כל הבעיות האלו, למה לבחור ברשת שוויונית? הסיבה פשוטה, רשתות אלו קלות ופשוטות ביותר להתקנה והפעלה. לרוב מספיקים מערכת ההפעלה הבסיסית וחיבורי הרשת הפיסיים. משתמשים בסביבה משרדית קטנה יצטרכו רק לחבר את המחשבים שלהם יחד ולהתחיל לשתף נתונים ומידע דרך הרשת. רשתות שוויוניות אינן דורשות הכשרת צוות מקיפה, הן גם אינן דורשות צוות תמיכה לשמירה על פעילות הרשת. מכיון שאין בקרה מרכזית, אם מחשב אחד נופל, כל המחשבים האחרים ברשת ממשיכים לתפקד. עבור עסקים קטנים רבים, זו עשויה להיות דרך פשוטה ויעילה לגישה לנתונים.

מספר דוגמאות של מערכות הפעלה שיכולות לפעול ברשת שוויונית כוללות את Microsoft Windows NT Server, Microsoft Windows NT Workstation, Windows 9x/ME, Windows 2000 Server, Windows 2000 Professional ומערכת ההפעלה Macintosh של Apple.



הערה: Windows NT Server **יכול לפעול ברשת מסוג** Peer-to-Peer **אם הוא יותקן בתור** member server. Windows 2000 Server **יכול לפעול ברשת מסוג** peer-to-peer **אם הוא יוגדר בקבוצת עבודה** (Windows 2000 Workgroup). **בקבוצת עבודה, מחשב הפועל תחת** Windows 2000 Server **נקרא מחשב** Stand-alone.



רעיון מפתח

ברשת שוויונית, יכול כל מחשב לשמש הן כשרת המשתף משאבים והן כלקוח המשתמש במשאבים.



טיפ: כדי להתגבר על בעיית חוסר השליטה, נוהגים לעיתים גם ברשת שוויונית לקבוע כללים לאחסנת הנתונים, כמו למשל הקצאת מחשב אחד למטרה זו. כך אפשר לשלוט באחסנה ובגיבוי בדרך נוחה יותר.

יתרונות רשתות שוויוניות

לרשתות שוויוניות יש יתרונות רבים, וביניהם :

- עד 10 משתמשים (זו אינה מגבלה טכנית אלא מגבלת ביצועים),
- קלות יחסית להתקנה,
- עלות נמוכה,
- אין צורך במחשבים נוספים או במוצרי תוכנה נוספים מעבר למערכת ההפעלה,
- בקרה מקומית על משאבים מבוצעת על ידי משתמשים,
- אין צורך בצוות מיוחד לתחזוקת הרשת,
- מחשבים בודדים אינם תלויים בתפקוד של מחשב מרכזי.

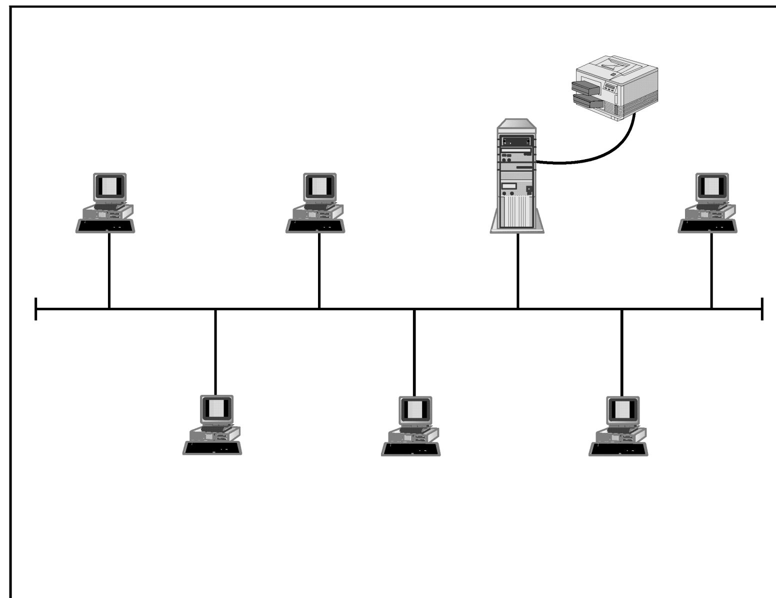
חסרונות רשתות שוויוניות

רשתות שוויוניות עשויות להתאים לסביבות עבודה קטנות, אולם יש להזכיר מספר חסרונות שלהן, וביניהם:

- ✯ אבטחת הרשת חלשה ומוגבלת להגנת סיסמה בלבד,
- ✯ משתמשים צריכים לזכור סיסמאות רבות, כדי לגשת למשאבי הרשת השונים,
- ✯ גיבוי נתונים המאוחסנים על מחשבים רבים מסובך ודורש זמן רב,
- ✯ יש ירידה בביצועי המחשבים בגלל הוספת העומס של שיתוף רשת,
- ✯ חוסר בסכימה ארגונית מרכזית - משתמשים צריכים לחפש מידע במחשבים רבים.

רשתות מבוססות שרת

רשתות מבוססות שרת (server based networks) מספקות בקרה מרכזית על משאבי הרשת, שלא כמו רשתות שוויוניות שנדונו קודם. רשתות מבוססות שרת מוכרות גם כרשתות **שרת/לקוח** (client/server) מכיון שהן מחלקות את המחשבים למחשבי לקוח ומחשבי שרת. כפי שניתן לראות בתרשים 1.8, מחשבי הלקוח משתמשים במשאבי הרשת ומחשבי השרת מספקים משאבים, אבטחה וניהול מערכת משותפים לרשת.



תרשים 1.8: *ברשת מבוססת שרת, מחשבי שרת מספקים בקרה מרכזית על משאבי הרשת*



הערה: שים לב שהמונח שרת/לקוח (Client/Server) יכול לשמש בהקשרים שונים. כאן הוא משמש לתיאור רשת, אולם ניתן להשתמש בו גם לתיאור היישומים הפועלים ברשת, כגון מערכות בסיסי נתונים ודואר אלקטרוני.

מחשבים המיועדים לשמש כשרתים עוברים אופטימיזציה לצורך שימוש ברשת על ידי הוספת מעבדים מהירים יותר, יותר זיכרון מערכת, כונני דיסק גדולים ומהירים יותר והתקנים נוספים כגון כונני טייפ וכונני תקליטורים, אלה בדרך כלל מתוכננים לאפשר למספר משתמשים לגשת בו-זמנית למשאבים משותפים. ברוב המקרים שרתים אינם משמשים לפעולות משרד כלליות, אלא רק לפעולות מיוחדות, כמו למשל אספקת גישה לקבצים משותפים. במקרים רבים השרת ימוקם בחדר נפרד בבניין, הרחק מאזור הצוות.

ברשת מבוססת שרת, כל חשבונות המשתמשים (רישומי המשתמשים) והסיסמאות מאושרים או מאומתים על ידי שרת מרכזי כלשהו. לדוגמה, ברשת Windows NT Server, משתמשים יכולים להיות חלק מ**תחום** (domain). לפני שמשתמש מקבל גישה למשאבים ברשת, **בקר התחום** (**DC** - **D**omain **C**ontroller) חייב לאמת את שם המשתמש ואת הסיסמה שלו. בקר התחום (DC) הוא אחד השרתים ברשת. רק מנהלי מערכת (System Administrators) יכולים לשנות את **זכויות הגישה** (access privileges) ולקבוע למי יש גישה למה. אבטחה ברשת מסוג זה יכולה להיות הדוקה מאוד.



הערה: ב-Windows NT היו שני סוגים של Domain Controllers. האחד נקרא PDC (Primary Domain Controller) והשני נקרא BDC (Backup Domain Controller). ב-Windows 2000 יש רק Domain Controller אחד הנקרא DC. ברשת Windows 2000 כל ה-DCs מתייחסים זה אל זה כשווים (Peers).

רשתות מבוססות שרת קלות יותר לשימוש מאשר רשתות שוויוניות מכיון שלמשתמשים אין סיסמאות רבות. קל יותר למצוא תוכניות וקבצים במרבית המקרים, מכיון שהם ממוקמים על שרתים מסוימים, ולא על מחשבים שונים המפוזרים ברחבי הרשת. ארגון מרכזי זה צורך פחות זמן עבודה לניהול ביחס לרשתות שוויוניות ומקל גם על גיבוי הנתונים.

יתרון חשוב נוסף לרשתות מבוססות שרת הוא יכולת הגידול. עם ניהול מרכזי של חשבונות לקוחות ושל הרשת, רשתות מבוססות שרת יכולות לגדול ממספר משתמשים בודדים לאלפי משתמשים, לפי הצורך.

את החיסרון העיקרי ברשתות מבוססות שרת ניתן לסכם במילה אחת - עלות. הן התוכנות והן חומרת השרת עלולות להיות יקרות מאוד. בנוסף, בדרך כלל נדרש **מנהל רשת** (network administrator), או **מינהלן רשת**, במשרה מלאה. משרה זו דורשת לרוב הכשרה נרחבת כדי שמנהל הרשת יוכל לבצע את עבודתו כהלכה.

בעיה נוספת היא תקלות בשרת. ברשת שוויונית, אם יש תקלה במחשב אחד, האחרים ימשיכו לפעול, אולם הם לא יוכלו לפנות אל המשאבים שנמצאים במחשב שכשל. ברשת מבוססת שרת, כשל במחשב שרת אינו רק אי-נוחות למשתמש מסוים, אלא עלול להשבית ("להפיל") את כל המערכת! ייתכן מצב שבו משתמשים אינם יכולים לגשת למשאבים, או אפילו לרשת עצמה.



רעיון מפתח

רשתות מבוססות שרת מספקות בקרה מרכזית על משאבי הרשת וסומכות על מחשבי השרת לספק אבטחה וניהול של הרשת.

יתרונות של רשתות מבוססות שרת

היתרונות של רשתות מבוססות שרת כוללים:

- ✯ בקרה מרכזית על אבטחה,
- ✯ ניהול פשוט למספר גדול של חשבונות משתמש,
- ✯ גישה מהירה יותר לקבצים/משאבים כתוצאה מביצוע תהליכי אופטימיזציה,
- ✯ קל יותר למשתמשים לגשת למשאבי רשת מכיון שהם צריכים לזכור רק סיסמה אחת.

חסרונות של רשתות מבוססות שרת

למרות יעילותם הרבה, יש לרשתות מבוססות שרת גם חסרונות, וביניהם:

- ✯ החומרה והתוכנה יקרות יותר,
- ✯ בדרך כלל נדרשים צוות נוסף והכשרה נוספת,
- ✯ אם שרת כושל, כל המערכת עלולה להיות בלתי שמישה.

רשתות משולבות

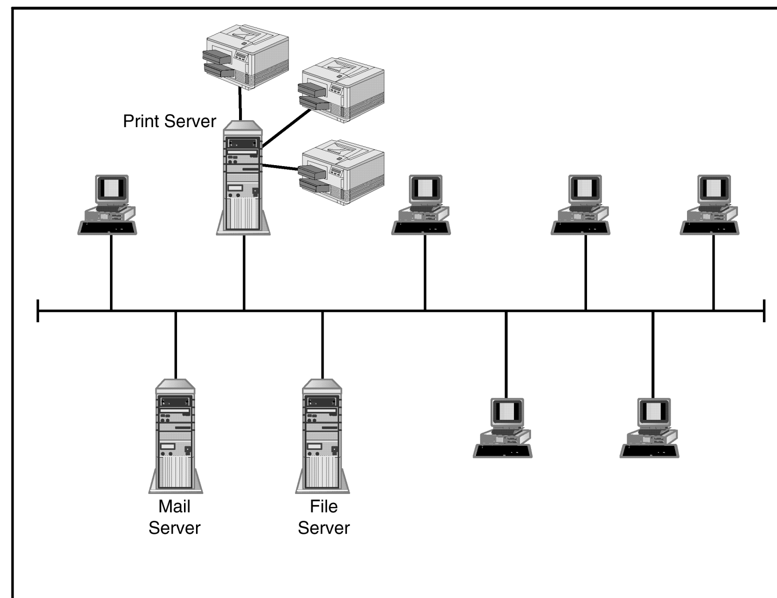
מערכות ההפעלה השולחניות כגון Windows 9x/ME, Windows NT Workstation ו-Windows 2000 Professional טשטשו את הקו המפריד בין רשתות שוויוניות (peer-to-peer) לבין רשתות שרת (server based). למעשה, נפוץ מאוד מצב של רשת מבוססת שרת שבה תחנות עבודה רבות של לקוחות מתפקדות כשוויוניות (peers).

תרחיש אופייני עשוי לכלול Windows 2000 Server רץ על שרתי הרשת, המספק אבטחה ואחסון של קבצים מרכזיים. משתמשי הרשת, אשר מריצים Windows 9x או Windows NT Workstation בתחנות, יקבלו הרשאת גישה לכל המשאבים המבוססים על השרתים, אולם יוכלו גם לשתף את הקבצים או את המדפסות שלהם.

לרשתות משולבות (combination networks) יש את רוב היתרונות של **שני** סוגי הרשתות. אולם החסרונות הם למעשה כמו של רשתות מבוססות שרת.

סוגי שרתים

במסגרת רשת מבוססת שרת, מחשבי השרת עשויים למלא תפקידים שונים. חלק מהשרתים יועדו לפעולה מסוימת אחת, ואחרים עשויים למלא מספר תפקידים שונים. לדוגמה, רשת כמו זו שבתרשים 1.9 יכולה לייעד מחשבי שרת להדפסה (עם מספר מדפסות), להעברת מסרי דואר (הודעות), ולאחסון קבצים.



תרשים 1.9: *רשת מבוססת שרת עשויה לכלול מחשבי שרת המיועדים למשימה מסוימת*

שרתי קבצים (File Servers)

כמעט בכל רשת תמצא שרת המשמש כמאגר מרכזי של קבצים. ניתן להתייחס לכך כאל המקביל האלקטרוני של חדר מלא מקיר לקיר בארונות תיוק. משתמשים יאחסנו את המסמכים, הגרפיקה, והקבצים האחרים שלהם בשרת זה. **שרתי קבצים** (file servers) הם אחת הסיבות העיקריות לרישות, ומהווים את המרכיב העיקרי של כל תוכנית רשת. אחסון מרכזי זה של נתונים מספק יתרונות רבים, וביניהם:

✫ **ארגון מרכזי**. במקום לחפש קבצים במחשבים רבים כמו ברשת שוויונית, יכולים המשתמשים לפנות ישירות לשרת הקבצים לחיפוש הנתונים.

✫ **אבטחת נתונים**. אם כל הקבצים נמצאים במקום אחד, קל יותר לגבות אותם להגנה מפני אובדן. שרת קבצים אופייני מחובר בדרך כלל להתקן גיבוי, כגון כונן טייפ, או כונן דיסק אופטי. גיבויים סדירים, המבוצעים בדרך כלל בכל יום, יכולים להבטיח שנתונים לא יאבדו כתוצאה מכשל בציוד.

✯ **מהירות**. שרתי קבצים הם לרוב מחשבים מהירים המריצים מערכת הפעלת רשת כגון Windows NT Server, או Novell NetWare, המיועדות במיוחד לניהול והפעלת שרת. מערכות הפעלה אלו עברו אופטימיזציה כדי לאפשר גישה מהירה לקבצים. בדרך כלל שרתים אלה גם מצוידים בכונני דיסק מהירים והתקני אחסון נוספים.

שרתי הדפסה (Print Servers)

יעד עיקרי נוסף להקמת רשת הוא שיתוף מדפסות. ברשת קטנה, מדפסת יכולה להיות מחוברת למחשב יחיד, ולהיות **משותפת** ברשת שוויונית באמצעות מערכת הפעלה כגון Windows 9x או Windows NT Workstation. משתמשים אחרים ידפיסו למדפסת זו באמצעות שירותי הרשת.

מצב זה מתאים לסביבת עבודה שהיקפה קטן. הבעיה מתעוררת כאשר גובר השימוש במדפסת. המשתמשים במחשב אליו מחוברת המדפסת יגלו שביצועי המחשב שלהם מואטים כאשר המדפסת בשימוש. בסופו של דבר מצב זה משפיע על התפוקה והיעילות של תחנת העבודה שלהם.

בנקודה זו, **שרת הדפסה** (print server), כפי שנראה בתרשים 1.9, יכול להיות פתרון מתאים. שרתי הדפסה הם בדרך כלל מחשבים ייעודיים שתפקידם הינו אספקת גישה למדפסות, ולרוב הם מנהלים מספר **תורי הדפסה** (print queues). כאשר משתמש מדפיס מסמך למדפסת מסוימת, הוא מועבר לתור ההדפסה המתאים למדפסת וממתין לתורו להדפסה. מנקודת מבטו של המשתמש, אין הבדל בין מצב זה לבין הדפסה למדפסת המחוברת ישירות למחשב שלו. המשתמש "מדפיס" את המסמך לתור ושרת ההדפסה עושה את כל השאר. יתרון נוסף הוא שהמסמך מועבר לשרת ההדפסה במהירות הרשת, ומאפשר למשתמש לחזור לעבודתו בזמן ששרת ההדפסה מטפל בתקשורת האיטית למדפסת.

בנוסף לפתרון בעיות מהירות, שרתי הדפסה גם מאפשרים ניצול יעיל יותר של המקום במשרד. ניתן למקם את המדפסות באזור מרכזי או בחדר נפרד, במקום להציבם ליד שולחן עבודה מסוים.

לשרתי הדפסה יש יתרון שהם מאפשרים שיתוף ציוד יקר בין כל המשתמשים. לדוגמה, מקובל להתקין מדפסת לייזר, מדפסת הזרקת דיו צבעונית ומדפסת לייזר צבעונית על שרת הדפסה יחיד לשירות הכל. בנוסף, מכיון שמכשירי מודם פקס מטופלים בדרך כלל באופן דומה למדפסות, ניתן להקים שירותי פקס מרכזיים באמצעות שרת ההדפסה.

שרתי תקשורת ודואר
(Communication/Message Servers)

הגידול בשימוש הרשתות לתקשורת פנימית, הביא למצב בו מייעדים מחשבים מסוימים לתפקיד **שרתי תקשורת ודואר** (communication/message servers).

- **דואר אלקטרוני (Electronic Mail).** מערכות אלו הפכו כה גדולות ומורכבות, עד שחלק מהן אינן יכולות להתקיים ללא שרת ייעודי. במיוחד במקרים שבהם רשתות מחוברות לאינטרנט, נפוץ מאוד מצב של שרת דואר המתקיים בעיקר לטיפול בתעבורת דואר אלקטרוני מול אתרים אחרים באינטרנט.
- **קבוצת עבודה או יישום קבוצת עבודה (workgroup or groupware).** תוכנות כגון Lotus Notes או Microsoft Exchange Server מציבות גם הן דרישות כבדות למשאבי חומרה. תוכניות מסוג זה מספקות יותר מדואר אלקטרוני פשוט וכוללות גם לוחות מודעות לדיון (discussion bulletin boards), יישומי זרימת עבודה (Work Flow), ובסיסי נתונים. במערכות תפעוליות גדולות, הן אינן יכולות להתקיים במשותף על מערכת המשמשת גם לשירותים אחרים.
- **שירותי אינטרנט (Internet publishing and Internet services).** גם אלה משחקים תפקיד גדול יותר בגיבוש סביבות הרשת בסביבה העסקית בה הכל מתקשר ודרך האינטרנט. לדוגמה, מיקרוסופט עם מערכת Internet Information Server - **IIS** וסדרת מוצרי Microsoft .NET.

Gateway Server

שירות המאפשר התקשרות של הרשת הארגונית עם רשתות אחרות העובדות (בארגון או מחוצה לו) עם פרוטוקולים אחרים. לדוגמה, מחלקת השיווק בארגון עובדת ברשת מחשבי PC המקושרת למחשב Main Frame בארגון לצורך שליפת נתונים, וכמו כן היא מקושרת למספר מערכות של לקוחות גדולים בעולם.

שרתי יישומים
(Application/Database Servers)

כאשר מתקינים במחשב יישום כגון Microsoft Office עושים זאת בדרך כלל בכונן הקשיח של המחשב, המסומן לרוב "C:". ללא רשת, גם הקבצים שלך יאוחסנו בדיסק הקשיח המקומי. עם הופעת הרשתות, רוב החברות החלו להשתמש בשרתי קבצים כאזור אחסון מרכזי. אולם מה לגבי היישומים היוצרים את אותם קבצים?

בסביבות מרושתות רבות, ממשיכים להתקין את היישומים (התוכניות השונות, כגון תוכנות Office, ניהול מלאי, הנהלת חשבונות ועוד) על הדיסקים הקשיחים המקומיים. בתרחיש זה, מכיון שקבצי ההגדרות (setup files) וקבצי ההרצה (executable files) הינם מקומיים, התעבורה ברשת מתרחשת רק כאשר המשתמש שומר, או קורא קובץ נתונים. הבעיה העיקרית בגישה זו היא - מה קורה כאשר יוצאת לשוק גירסה חדשה

של התוכנה? בדרך כלל מנהל הרשת צריך לעבור בין כל מחשבי הלקוח ולהתקין בהם את הגירסה החדשה.

כדי לפתור מצב זה, מנהלי רשת רבים נוהגים למקם את כל תוכנות היישום בשרת קבצים, ולא במקום כלשהו ברשת. כלומר, לשרת הקבצים נוסף תפקיד של **שרת יישומים** (application server). כאשר משתמש לוחץ לחיצה כפולה על סמל שעל שולחן העבודה שלו, או בוחר תוכנית מתפריט, קבצי ההרצה נקראים משרת הקבצים אל המחשב המקומי של המשתמש ומורצים בו. בגישה זו, קל מאוד למנהלי הרשת להתקין גירסה חדשה של התוכנה. הם משדרגים את הגירסה הנמצאת על שרת הקבצים בלבד, וכאשר משתמשים מפעילים שוב את היישום, הם יקבלו את התוכנה בגרסתה המעודכנת.



הערה: את רוב היישומים לא ניתן להתקין על שרת קבצים לשימוש כל משתמשי הרשת. במקרים רבים יש לרכוש גרסת רשת (network version) של התוכנה, או לפחות לרכוש רשיון לקוחות (client license) המכסה כל אחד מהמשתמשים שישתמש בתוכנה.

למרות ששיטה זו פועלת, ככל שיותר אנשים משתמשים ביישומים משרת הקבצים, פוחתת המהירות שבה הם יכולים לגשת למסמכים ולקבצים אחרים משרת קבצים זה. כתוצאה מכך, ברשתות גדולות, ייתכן מצב שבו כל תוכנות היישומים נמצאות במרוכז על **שרת יישומים** (application server) נפרד, וכל קבצי הנתונים ימשיכו להיות על שרת קבצים.

בנוסף להגברת מהירות הגישה לקבצי נתונים משרת הקבצים, הפרדת היישומים בדרך זו מספקת שני יתרונות נוספים למנהלי הרשת. כאשר מנהלי הרשת רוצים לשדרג יישומים, קל לאתר את הגירסה הישנה. בנוסף, שרת יישומים מרכזי מגביר את היעילות של גיבויי נתונים יומיים. בעוד שיש לגבות קבצי נתונים בתדירות גבוהה יחסית, אין צורך לעשות זאת לקבצי יישומים, אשר בדרך כלל אינם משתנים וניתן לגבות אותם בתדירות נמוכה יותר.

שרתי יישומים הופכים נפוצים יותר בארגונים המשתמשים בתוכניות בסיסי נתונים גדולים. לעיתים שרתים אלה גם נקראים **שרתי בסיס נתונים** (database servers).

תווך רשת

תווך הרשת (network media) הוא למעשה המנגנון הנושא פיסית מסרים (הודעות) ממחשב למחשב. במונחים של העולם הפיסי, ניתן לחשוב על סוגי התווך השונים שבהם אנו משתמשים לתקשורת בין אנשים. אם ברצונך להעביר מסר למישהו, תוכל לכתוב מכתב, להתקשר אליו בטלפון, לשלוח פקס או דואר אלקטרוני. אם באמת ברצונך להעביר מסר לאדם שקשה להשיגו, תוכל לשדר אותו בטלוויזיה, לפרסם מודעה בעיתון, או לקשור שלט למטוס! כל המנגנונים האלה הם ה**תווך** (media) שבעזרתו אנו מתקשרים.

בעולם של רשתות מחשבים, קיימים שלושה סוגים שונים של תווך :

- ✯ חוטי נחושת (copper wire),
- ✯ סיבים אופטיים (fiber-optics),
- ✯ טכנולוגיות אלחוט (wireless technologies).

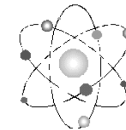
תרשים 1.10 מציג דוגמאות של תווך אלחוטי.

נחושת

נחושת (copper) היא תווך תקשורת עיקרי לרישות מחשבים. היא הרכיב העיקרי של מעגלים חשמליים פנימיים. נחושת נמצאת בשימוש למטרה זו למעלה ממאה שנה, ומאפייניה ויכולותיה מוכרים וידועים. השיטה שבה חשמל זורם דרך נחושת נחקרה לעומק. הנחושת אומצה לצרכים חשמליים רבים. רוב כבלי הרשת מכילים ציר נחושת מרכזי כמו למשל כבלי טלפון וטלוויזיה.

סיבים אופטיים

עם כל יתרונותיה של הנחושת, היא אינה יכולה להשתוות למהירות האור. כבלי סיבים אופטיים (fiber optics) מורכבים מסיבים אופטיים העשויים מזכוכית או מפולימרים פלסטיים שונים, אשר הם בעלי תכונות פיסיקליות וכימיות המאפשרות הלוכה והזרמת האור למרחקים. הסיבים האופטיים מעבירים אלומות אור. אלומות אור אלו יכולות לשאת אות על פני מרחק רב יותר מאשר כבלי נחושת, והן אינן מושפעות מהפרעות רדיו, או הפרעות אלקטרומגנטיות אחרות.



על ה- Web

פרטים נוספים על סיבים אופטיים תוכל למצוא באתר

http://www.mcs-israel.co.il/

החיסרון העיקרי של סיבים אופטיים הוא העלות הגבוהה של הכבלים ושל ציוד הנחוץ לתמסורת הנתונים (data transmission).

בשל העלות הגבוהה, משמשים סיבים אופטיים בדרך כלל **כאפיקי שידרה** (backbones) של רשתות או בין רשתות. ניתן גם למצוא סיבים אופטיים באזורים המושפעים מהפרעות אלקטרומגנטיות רבות. הפרעות מסוג זה עלולות לעוות את האות החשמלי בכבל נחושת, אולם לא יפריעו לאות האור בסיב אופטי.

אלחוט

תווך רשת אלחוט (wireless network media) כולל למעשה מספר טכנולוגיות שונות. המשותף להן הוא שאין צורך בכבל פיסי כלשהו. קיימים שלושה סוגים של טכנולוגיות אלחוט המקובלות כיום בשימוש : אינפרא-אדום, מיקרוגל ורדיו.

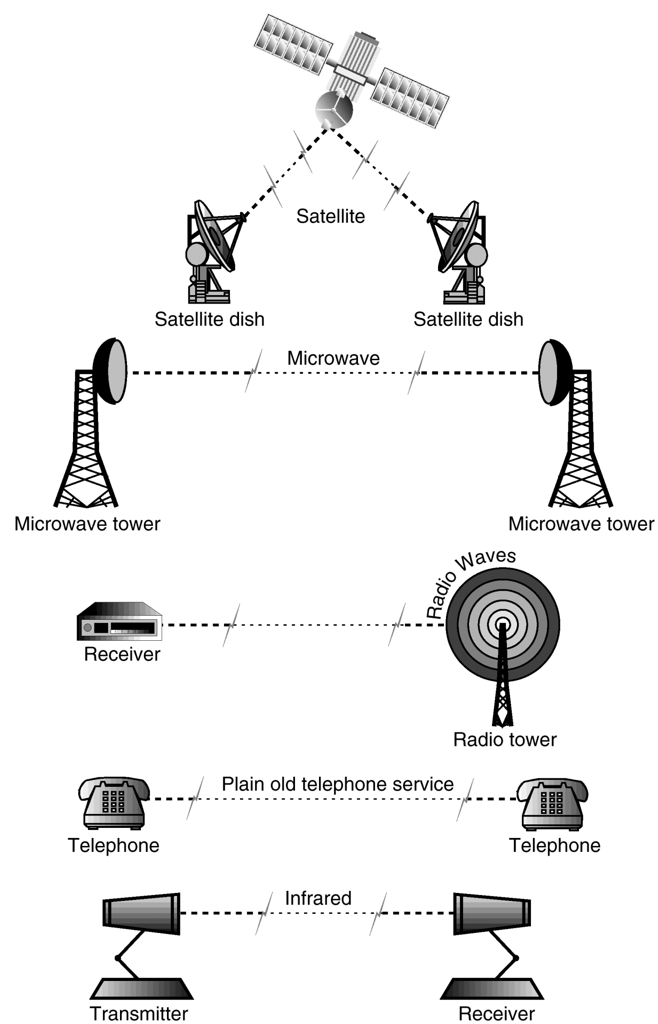
רשתות **אינפרא-אדום (infrared)** נפוצות במתחם משרדי מוגבל, שבו האותות אינם צריכים לעבור מרחק רב. לדוגמה, אם אתה איש מכירות בחברה וסדר היום שלך כולל כניסות ויציאות רבות מהמשרד במשך היום, תוכל להשתמש במחשב נישא בעל מתאם אינפרא-אדום. כאשר אתה חוזר למשרד, אתה מניח את המחשב הנישא על שולחן העבודה שלך ומכוון את המתאם אל כניסת אינפרא-אדום שבמחשב האישי שעל שולחנך. כך המחשב הנישא שלך מתחבר מיידית לרשת. עם צאתך, אתה לוקח את המחשב הנישא שלך ועוזב. אין צורך להתעסק כלל עם כבלים או כרטיסי רשת.

הבעיה ברשתות אינפרא-אדום היא בכך שהן בדרך כלל מוגבלות **לקו ראייה** (line-of-sight). פירוש הדבר שמתאם הרשת על המחשב צריך "לראות" את כניסת הרשת המתאימה שלו. בגלל ריהוט משרדי וציוד אחר העלול לחסום קו ראייה זה, רשתות אינפרא-אדומות אינן מעשיות במשרדים רבים, והשימוש בהן מוגבל לטווח קצר בלבד.

רשתות אינפרא-אדום גם איטיות ומוגבלות בטווח. רשתות אופייניות פועלות בפחות מחצי ואפילו פחות מעשירית המהירות של רשת נחושת מקבילה וטווח העבודה שלהן אינו עולה על תשעה מטרים (30 feet).

רשתות **מיקרוגל (microwave)** משמשות בעיקר לחיבור בין רשתות על פני מרחקים גדולים, או באזורים שלא ניתן להשתמש בהם בכבלים. למרות שתקשורת מיקרוגל מחייבת "קו ראייה" בדומה לאינפרא-אדום, היא יכולה לכסות מרחקים גדולים הודות לתדרים שהיא משתמשת בהם. רשתות מיקרוגל עשויות להשתמש בסדרה של מגדלי ממסר על פני הקרקע להעברת המסרים, או להשתמש בלוויינים לשידור האותות לחלק אחר של כדור הארץ. החיסרון העיקרי של רשתות מיקרוגל הוא בכך שהן מושפעות מתנאי מזג האוויר כמו גשם, או ערפל.

רשתות **רדיו (radio)** הולכות ונעשות נפוצות יותר עם התפתחות טכנולוגיות תקשורת חדשות. גלי רדיו יכולים לחדור דרך קירות, הם עמידים בתנאי מזג אוויר משתנים, ובעזרת מערכות לווין חדשות הם יכולים להגיע למרבית המקומות על פני כדור הארץ. יכולות ותכונות אלו ימלאו ללא ספק תפקיד חשוב ברשתות העתיד. טכנולוגיות איתור (paging) וטכנולוגיות תאיות (סלולריות, cellular) חדשות מציעות גם הן אפשרויות מתקדמות. המחסומים העיקריים בשעה זו להרחבת השימוש ברדיו הם עלות הרשתות והחוסר בתדרים אלקטרומגנטיים שבהם ניתן לפעול. אולם, עם התפתחות פתרונות פוליטיים וטכנולוגיים, כדאי לבחון סוג זה של רשת כדי להמשיך לצמוח.



תרשים 1.10: *קיימות צורות רבות של תווך אלחוטי*

סיכום

רשתות מחשבים יכולות לפתור בעיות עסקים אמיתיות, ולהגדיל את התפוקה והיעילות הכוללות של הארגון.

בכל פעילות בין מחשב אחד לבין מחשב אחר ברשת, מחשב מתפקד כ**לקוח** (client) בעת שימוש במשאבים ממחשב אחר, או כ**שרת** (server) בעת שיתוף משאבים עם מחשבים אחרים.

שני סוגי הרשתות העיקריים הם רשתות **שוויוניות** (peer-to-peer) ורשתות **מבוססות שרת** (server based). ברשתות **שוויוניות**, כל המחשבים שווים במובן שאין בקרה מרכזית על המשאבים. כל מחשב יכול לשמש הן כלקוח והן כשרת. ברשתות **מבוססות שרת**, גישה למשאבים מבוקרת באופן הדוק. המשאבים גם יכולים להיות מרוכזים ומאורגנים באופן יעיל.

ברשת **מבוססת שרת**, עשויים להיות מספר סוגים שונים של שרתים במחשבים שונים, או שמחשב אחד יכול למלא מספר תפקידי שרת. שרתי קבצים מספקים אזור אחסון מרכזי לקבצים. שרתי הדפסה מאפשרים שיתוף פשוט ונוח של מדפסות והתקנים דומים אחרים. שרתי תקשורת מיועדים לאספקה יעילה של שירותי דואר אלקטרוני או שירותי יישומים לקבוצות עבודה.

בסופו של דבר, רשתות מחשבים עוסקות בהעברת נתונים על פני **תווך** פיסי. ה**תווך** (media) המשמש ברשת עשוי להיות נחושת, סיבים אופטיים, או טכנולוגיות אלחוט כגון רדיו, מיקרוגל ואינפרא-אדום.

2

מודל הייחוס OSI

פרק זה מציג את **מודל הייחוס OSI** (Open Systems Interconnection Reference Model) שישמש כמסגרת לדיון במהלך הלימוד בספר זה. מודל OSI (כך נכנה אותו בקיצור) יתואר בפירוט בהקשר התיאורטי ובהקשר של העולם האמיתי.

נושאי פרק זה כוללים:

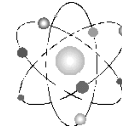
- ✯ מסגרת תפישתית,
- ✯ שבע השכבות של מודל הייחוס OSI,
- ✯ שיפורי IEEE למודל OSI,
- ✯ יישום מודל OSI.

מסגרת תפישתית

בסוף שנות ה-70, **ארגון התקינה הבינלאומי - ISO** (International Standards Organization) החל לפתח מודל רשת תיאורטי. בשנת 1978, הארגון פרסם את הגירסה הראשונה של מה שהוכר אחר כך **כמודל ייחוס OSI** (Open Systems Interconnection Reference Model). בשנת 1984, פורסמה גירסה חדשה שהפכה לתקן בינלאומי ולבסיס למרבית הדיונים בנושאי רישות (networking).



הערה: המונח מערכות פתוחות (open systems) מתייחס לכך שהמודל תוכנן במטרה לאפשר חיבורים בין מערכות מחשבים שונות. כך הוא אינו מוגבל על ידי מערכות קנייניות של ספק כלשהו.



גלו ה- Web

אתה מוזמן לבקר באתר הארגון בכתובת http://www.ldcs.org/iso.htm

רישות בשכבות

מודל ייחוס OSI מתאר תקשורת מרושתת כסדרה של **שכבות** (layers). כדי להבין את העקרונות של תקשורת בשכבות, נבחן דוגמה של תקשורת בעולם הפיסי.

נניח כי משה הוא מנהל בחברה גדולה בעיר אחת שרוצה לשלוח מסמך לשרה, מנהלת באותה חברה הנמצאת בעיר אחרת.

תרחיש אפשרי בקצה שבו נמצא משה יכול להיות כזה:

1. משה כותב או מכתיב מסמך ומעביר אותו לעוזר שלו.
2. העוזר מדפיס את המכתב.
3. העוזר מכניס את המסמך לתוך מעטפת דואר בין משרדי, כותב עליה כתובת, ומשאיר אותה לאיסוף.
4. פקיד הדואר הפנימי אוסף את המעטפה ומעביר אותה לחדר הדואר.
5. צוות חדר הדואר קורא את הכתובת וקובע אם המעטפה מיועדת ליעד מקומי, או ליעד כלשהו אחר.
6. הצוות קובע גם כיצד יש להעביר את המעטפה: אם על ידי שליח או על ידי שירות דואר מהיר.
7. הצוות מכניס את המעטפה למעטפה אחרת על פי השירות שנבחר לשיגור.
8. הצוות ממלא את הטפסים הדרושים, קובע את המחיר, ואת אפשרויות התשלום המתאימות.
9. צוות השירות שנבחר מטפל באיסוף החבילה.

בשלב זה החבילה נכנסת לרשת של ספק התעבורה. ברוב המקרים, היא מועברת למרכז ואז למתקן אזורי, ובו היא מוכנסת למשאית כלשהי הנוסעת לאתר של שרה.

כעת נבחן את התהליך בקצה שבו נמצאת שרה:

1. החבילה נמסרת לחדר הדואר במתקן שבו נמצאת שרה.
2. צוות חדר הדואר מסיר את המעטפה החיצונית.
3. הצוות קובע למי הדואר מיועד וממיין אותו לערימה המתאימה לאספקה.
4. פקיד הדואר לוקח את הדואר לאזור המשרד של שרה, ומתחיל לחלק מעטפות.
5. המעטפה של משה מועברת ביחד עם דואר אחר לעוזר של שרה.
6. העוזר פותח את המעטפה ובוחן את החומר.
7. בסיום, המסמך של משה מגיע לשרה.

כל הצעדים הללו נחוצים לאספקת המסמך מהמקור ליעד. ואכן, בגישה שכבתית זו, מסמכים מועברים ממשרד למשרד. שים לב שיש תהליך המבוצע בשני הקצוות של מסלול התקשורת. מספר שכבות היו מעורבות לפני שהמסמך הגיע לספק התעבורה ובאופן דומה, היו מספר שכבות של תהליך לאחר שהחבילה הגיעה למשרד היעד.

שבע השכבות של מודל ייחוס OSI

מודל OSI מחלק את התקשורת ברשת מחשבים לשבע שכבות :

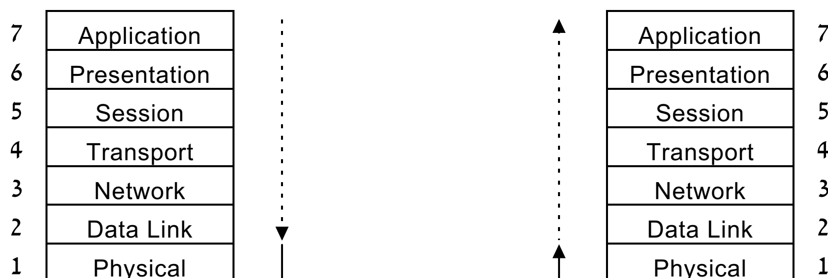
7	Application	יישום
6	Presentation	הצגה
5	Session	שיח
4	Transport	העברה
3	Network	רשת
2	Data Link	קישור נתונים
1	Physical	פיסית

תרשים 2.1: *מודל ייחוס OSI הוא בן שבע שכבות*

בראש המודל **בשכבת היישום** (Application Layer) נמצאות התוכניות המופעלות על ידי משתמשי המחשבים. תוכנית מסוג זה יכולה להיות תוכנת דואר אלקטרוני, תוכנית בסיס נתונים, או משהו בסיסי כמו מנהל הקבצים או סייר חלונות. בתחתית נמצאת **השכבה הפיסית** (Physical Layer) המורכבת מתווך הרשת המבצע את החיבור הפיסי בין המחשבים. בין שתי שכבות אלו נמצאות כל השכבות הגורמות לתקשורת להתרחש.

לפני הדיון בשכבות השונות, עליך להבין מעט יותר כיצד המודל פועל.

כאשר יישום (בשכבת היישום) שולח נתונים ממחשב אחד לאחר, הנתונים מועברים "מטה" בשכבות המודל. בעזרת השכבה הפיסית הם מועברים על פני הרשת אל השכבה הפיסית במחשב המקבל. משכבה זו במחשב המקבל הנתונים עוברים כלפי "מעלה" דרך שכבות המודל, עד שהם מגיעים אל שכבת היישום המצפה להם. קשר זה מוצג בתרשים 2.2.



תרשים 2.2: *כאשר שני מחשבים מתקשרים, הנתונים עוברים "מטה" דרך כל שכבות המודל, עוברים ברשת התקשורת, ו"עולים" בשכבות המודל של המחשב המקבל*

התהליך עצמו מעט יותר מסובך. למעשה, בכל שכבה של התהליך בקצה השולח נוסף לנתונים מידע כותרת. בקצה המקבל, אותן כותרות מוסרות, עד שבסוף הנתונים זמינים ליישום המקבל ללא כל תקורה.

כל שכבה יכולה לתקשר **רק** עם השכבה שמעליה או עם זו שמתחתיה. בקשה ממחשב אחד לקבלת קובץ הנמצא במחשב אחר **חייבת** לעבור מטה דרך כל השכבות שבמחשב השולח, ואחר כך לעלות דרך כל השכבות במחשב המקבל. כל שכבה יודעת כיצד להעביר את הנתונים לשכבה שמעליה או מתחתיה בלבד, אבל אינה יודעת (וגם לא צריכה לדעת) כיצד הנתונים מועברים הלאה, אל השכבות האחרות.

מי שמוביל את הנתונים ברשת הוא הפרוטוקול. כל עוד שני המחשבים המחוברים מדברים האותה שפה (פרוטוקול) אין בעיה, אבל כאשר שני מחשבים מוגדרים לפעול בשני סוגים שונים של פרוטוקולים. אם מחשב אחד משתמש ב- IPX/SPX ומחשב אחר משתמש ב- TCP/IP, לא תתקיים כל תקשורת ביניהם.



הערה: ניתן להפעיל מספר פרוטוקולים על מחשב יחיד. **לדוגמה,** מחשב **יכול** להריץ TCP/IP **כדי לתקשר עם האינטרנט ותחנות עבודה** UNIX**, ויכול גם להריץ** IPX/SPX **כדי לתקשר עם שרתי הקבצים של** Novell.

שכבת היישום (Application)

שכבת היישום (Application Layer) אחראית לקישור היישום עם הרשת ללא תלות בסוג הרשת. בראש מודל OSI נמצאת **שכבת היישום** שעסוקה בעיקר באינטראקציה בין המשתמש למחשב. שירותים ברמה זו תומכים ביישומי משתמשים כמו דואר אלקטרוני, שאילתות לבסיסי נתונים, והעברת קבצים.



רעיון מפתח

בשכבת היישום (Application Layer), **נמצאים יישומי משתמשים שמתקשרים** עם הרשת.

שכבת ההצגה (Presentation)

שכבת ההצגה (Presentation Layer) אחראית לתרגום הנתונים לפורמט מוכר, להצפנה ופיענוח וברשתות מיקרוסופט להצגת הנתונים המרוחקים כמשאבים מקומיים על ידי Redirector service.

שכבת ההצגה מבצעת מספר פעולות עם הנתונים. הפעולה העיקרית שלה היא לקחת את הנתונים משכבת היישום (Application Layer) ולתרגם אותם לתצורה המובנת לכל סוגי המחשבים.

שכבת ההצגה אחראית על הצפנה, אם נעשת. הודעות יוצאות מוצפנות (Encrypt) לצורך ההעברה, והודעות נכנסות מפוענחות (Decrypt) עבור ההצגה לשכבת היישום.

לסיום, שכבת ההצגה עשויה להפעיל סוג כלשהו של דחיסת נתונים, כדי להקטין את נפח הנתונים לקראת המעבר ברשת.



הערה: ברשתות מיקרוסופט פועל בשכבה זו שירות שנקרא redirector (מנתב מחדש). הנתב הזה מציג מידע רשת ליישומים הפונים למשאבי רשת מתוך שכבת היישום. לדוגמה, כאשר אתה נמצא במנהל הקבצים או בסייר חלונות, ורוצה לראות את רשימת הספריות של תיקייה בשרת, מנהל הקבצים מבקש בקשה כמו זו שהיתה מוצגת לדיסק קשיח מקומי; אך כאן, בקשה זו מנותבת (redirected) אל השרת המתאים ברשת. הנתב לוכד את הבקשה ומעביר אותה ברשת. נתב זה גם מטפל בבקשות הדפסה ברשת (מעביר את הפלט אל המדפסת המיועדת).



רעיון מפתח

חשוב על שכבת ההצגה (Presentation Layer) כשכבה המכינה את הנתונים לתצוגה ברשת (אם הם בדרכם החוצה), או לתצוגה ליישומים (אם הם בדרכם פנימה).

שכבת השיח (Session)

שכבת ה- Session אחראית לפתיחת ה-Session (פעולה בין שני מחשבים) וסגירתו וכן על העברת הנתונים כולל נקודות בדיקה וביקורת ובכך היא קובעת חוקים להעברת נתונים.

בדרך כלל תרצה להעביר כמויות גדולות של נתונים, אולם אתה גם רוצה שאחרים יוכלו להשתמש ברשת באותו זמן. כדי לפתור בעיה זו, "שוברות" הרשתות את הנתונים ל**מנות** (packets) קטנות לצורך השידור ברשת. כאשר אתה שומר מסמך גדול בדיסק של שרת הקבצים ברשת, הקובץ לא נשלח ברשת כגוש גדול אחד. למעשה הוא מחולק למספר רב של מנות קטנות הנשלחות בנפרד.

המחשב המקבל חייב לדעת בדרך כלשהי, היכן מתחילה ההעברה והיכן היא נגמרת. תפקיד זה מבוצע על ידי שכבת ה-Session. כאשר אתה רוצה לשמור את המסמך, המחשב מסמן לשרת הקבצים שהוא רוצה לפתוח Session עם השרת. אם הרשאות האבטחה מאשרות זאת, הקשר יתחיל. לאחר שמירה מוצלחת של המסמך, שכבת ה-Session מסמנת שההעברה היתה מוצלחת ומסיימת את הקשר.

שכבת ה-Session גם מבצעת פעולה חשובה על ידי הצבה ובדיקה של **נקודות ביקורת** (checkpoints) בזרם הנתונים במהלך שיגור הנתונים. אם יש תקלה זמנית ברשת, המחשב השולח יצטרך לשלוח מחדש רק את הנתונים שנשלחו לאחר נקודת הביקורת האחרונה.



רעיון מפתח

זכור את שכבת Session כפותחת, מבצעת, ומסיימת Session בין שני מחשבים.

שכבת ההעברה (Transport)

שכבת ההעברה (Transport Layer) אחראית לחלוקת הנתונים למנות (packets), מספור המנות ואריזתן מחדש לנתונים. היא למעשה מבצעת את החוקים שנקבעו על ידי שכבת ה-Session.



רעיון מפתח

זכור את **שכבת ההעברה** (Transport Layer) כשכבה המבטיחה העברת נתונים ללא שגיאות ובסדר הנכון.

שכבת הרשת (Network)

שכבת הרשת (Network Layer) אחראית לניתוב התעבורה ותרגום שמות לוגיים לפיסיים ולהיפך (Routers פועלים בשכבה זו). היא מתפקדת בדומה לחדר דואר.

ניתוב זה של הודעות לכתובות הוא האחריות העיקרית של **שכבת הרשת** (Network Layer) ברשת מחשבים. שכבת הרשת אחראית לרישום הכתובת של המסר ולקביעת הנתיב הטוב ביותר על סמך תעבורת רשת, רמות עדיפות ותנאים אחרים.



רעיון מפתח

זכור, **שכבת הרשת** (Network Layer) מנתבת מסרים לכתובת המתאימה בדרך הטובה ביותר האפשרית.

שכבת קישור הנתונים (Data Link)

שכבת קישור הנתונים (Data Link Layer) אורזת את המנות לחבילות ומבצעת מעקב וביקורת. שכבה זו גם אחראית על בקרת הגישה לתווך (Bridges פועלים בשכבה זו).

בשכבת קישור הנתונים כל המנות שנשלחו מהשכבות העליונות יותר מוכנסות ל**מסגרות נתונים** (data frames) כדי שיותאמו להעברה על ידי השכבה הפיסית. בנוסף למידע כותרת, שכבה זו בדרך כלל מוסיפה סיומת **CRC** (Cyclical Redundancy Check), שהמחשב המקבל יכול להשתמש בה כדי לבדוק ולוודא שהנתונים התקבלו בשלמות, כפי שמוצג בתרשים 2.3.

שכבת קישור הנתונים אחראית להבטיח שהמסגרות מתקבלות ללא שגיאות. לאחר משלוח המסגרת, השכבה מחכה לאישור מהמקבל. אם לא מתקבל אישור, המסגרת נשלחת שוב.



***תרשים 2.3:** בשכבת קישור הנתונים מתוספת בדיקת CRC למסגרת הנתונים*

בקצה המקבל, שכבת קישור הנתונים אחראית לזיהוי ייחודי של המחשב ברשת (בדרך כלל באמצעות כתובת המקודדת בכרטיס מתאם הרשת). כאשר היא מזהה מנה שנכנסת לכתובת שלה, היא מרכיבה את כל הסיביות מהשכבה הפיסית למסגרת, מאמתת את ה-CRC כדי לוודא את שלמות המנה, ואז מעבירה את המנה מעלה, אל שכבת הרשת. אם בדיקת CRC כושלת, שכבה זו תבקש העברה חוזרת של המנה.

שכבה זו אחראית גם לבקרה על איזה מחשב יכול לפנות לחיבור הרשת הפיסי בכל רגע. כפי שתוכל לשער, אם כל המחשבים ברשת יתחילו להעביר נתונים בו-זמנית, יהיה קשה מאוד לדעת אילו נתונים שייכים למי.

התקן הנקרא **מגשרים** (bridges) פועל בדרך כלל בשכבה זו, לשילוב חלקים שונים של רשת לרשת גדולה אחת.



רעיון מפתח

זכור את **שכבת קישור הנתונים** (Data Link Layer) כשכבה האורזת נתונים למסגרות, ומספקת קשר נטול שגיאות בין שני מחשבים.

השכבה הפיסית (Physical)

שכבה זו מגדירה את טופולוגיית הרשת (repeaters פועלים בשכבה זו). תקשורת רשתות המחשבים מסתכמת בספרות אפס (0) ואחד (1), שהם פולסים חשמליים העוברים בתווך התקשורת (network media). **בשכבה הפיסית** (Physical Layer), הנתונים מתורגמים לסיביות שיועברו דרך התווך הפיסי המשמש לחיבור בין המחשבים. במחסנית הפרוטוקול, שכבה זו מגדירה את התווך המשמש לחיבור, ואת אופן החיבור שלו למחשב (לדוגמה, כמה פינים דרושים במחבר הפיסי). שכבה זו מגדירה את מתח החשמל הדרוש וכל סוג אחר של קידוד להמרת הסיביות לאותות חשמליים.

לרוב הרשתות התקנים כמו **רכזות** (hubs), **מגברים** (repeaters), ויחידות **מקלט/משדר** (transceiver) הפועלים ברמה זו.

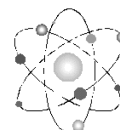


רעיון מפתח

זכור את **השכבה הפיסית** (Physical Layer) כחיבור הפיסי בין המחשבים.

שיפורי IEEE 802 למודל OSI
(תקנים סטנדרטיים לממשק הרשת)

במקביל לפיתוח מודל ייחוס **OSI** (Open Systems Interconnection) על ידי ארגון התקינה הבינלאומי - ISO (International Standards Organization), עסק גם ארגון IEEE (Institute of Electrical and Electronics Engineers) בתהליך פיתוח תקנים לכרטיס ממשק הרשת ולחיבור הפיסי. מאמץ זה הוכר כ**פרויקט 802** (על שם השנה והחודש שבו הוא החל - פברואר 1980).



על ה- Web

אתה מוזמן לעיין באתר ארגון IEEE בכתובת http://www.ieee.org

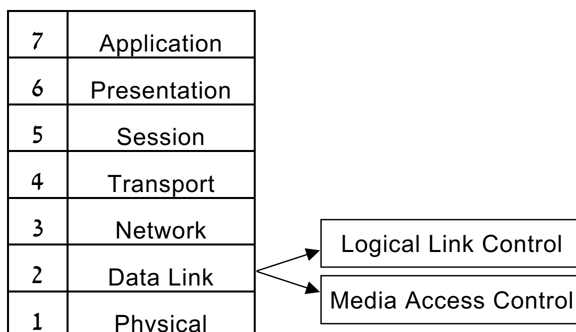
פרויקט IEEE הניב את **מפרטי 802** (802 specifications), המגדירים את הדרך שבה הנתונים משודרים על תווך הרשת הפיסי באמצעות כרטיסי ממשק הרשת (network interface cards). התקנים מתחלקים ל-12 קטגוריות, כפי שמוצג בטבלה 2.1.

מספר	קטגוריה
802.1	Internetworking
802.2	Logical Link Control (LLC)
802.3	Carrier-Sense Multiple Access with Collision Detection LAN (CSMA/CD or Ethernet)
802.4	Token-Bus LAN
802.5	Token-Ring LAN
802.6	Metropolitan Area Network (MAN)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrate Voice/Data Networks
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority Access LAN, 100 Base VG-AnyLAN
802.14	Cable television / Cable modems

טבלה 2.1: *מפרטי 802 של IEEE*

IEEE ביצעה שיפור חשוב למודל OSI. המהנדסים חשו ששכבת קישור הנתונים (Data Link) היתה זקוקה להבהרה נוספת וחילקו אותה לשתי תת-שכבות (ראה תרשים 2.4):

- **בקרת קישור לוגי** - LLC (Logical Link Control)
- **בקרת גישה לתווך** - MAC (Media Access Control)



תרשים 2.4: *פרויקט 802 של IEEE חילק את שכבת קישור הנתונים של מודל OSI לשתי תת-שכבות*

תת-השכבה בקרת קישור לוגי (LLC)

תת-השכבה **בקרת קישור לוגי** (LLC - Logical Link Control) אחראית לתחזוקת הקישור בין שני מחשבים כאשר הם שולחים נתונים על פני החיבור הפיסי של הרשת. היא עושה זאת על ידי יצירת סדרה של **נקודות שירות גישה** - SAPs (Service Access Points). מחשבים אחרים יכולים להשתמש בהן כדי לתקשר עם השכבות הגבוהות יותר של מחסנית פרוטוקול הרשת. המפרט העיקרי לתת-שכבה זו הוא 802.2.

תת-השכבה בקרת גישה לתווך (MAC)

באופן בסיסי, תת-השכבה **בקרת גישה לתווך** -**MAC** (Media Access Control) מאפשרת למחשבים ברשת לשלוח נתונים לפי התור על פני תווך הרשת הפיסי. תת-שכבה זו קובעת את השיטה לפיה מחשב קובע אם הוא יכול לשלוח מנה אל הרשת. תת-השכבה גם אחראית להבטיח שהנתונים יגיעו למחשב האחר ללא שגיאות. מפרטי IEEE העיקריים לתת-שכבה זו מוצגים בטבלה 2.2.

מספר	קטגוריה
802.3	Carrier-Sense Multiple Access with Collision Detection LAN (CSMA/CD or Ethernet)
802.4	Token-Bus LAN
802.5	Token-Ring LAN
802.12	Demand Priority Access LAN

טבלה 2.2: *קטגוריות 802 עבור בקרת גישה לתווך*

יישום מודל OSI בעולם המעשה

בעוד שמודל ייחוס OSI מספק מסגרת תיאורטית לדיון ברשתות מחשבים, במציאות מרבית מחסניות הפרוטוקול (אוסף של פרוטוקלים, למשל TCP/IP הוא אוסף שכזה) אינן מתאימות את עצמן לשבע שכבות ברורות ומסודרות. הרעיון השכבתי עדיין קיים, אולם במציאות אין פרוטוקול או מחסנית פרוטוקולים המיישמים אחד לאחד את המודל התיאורטי.

סיכום

מודל ייחוס OSI מהווה מסגרת שבה ניתן לתאר רשתות מחשבים ולהשוות בין הפעולות של מחסניות פרוטוקול שונות המשמשות ברישות. מודל OSI מחלק את תקשורת הרשת לשבע שכבות:

1. **יישום** (Application). מספקת קישורי רשת עבור יישומי משתמשים.
2. **הצגה** (Presentation). מכינה את הנתונים להעברה ברשת.
3. **שיח** (Session). מקימה שיח בין שני מחשבים.
4. **העברה** (Transport). מבטיחה תעבורת נתונים ללא שגיאות ובסדר הנכון.
5. **רשת** (Network). רושמת כתובות על מנות נתונים וקובעת את הנתיב הטוב ביותר אל היעד.
6. **קישור נתונים** (Data Link). אורזת נתונים לתוך מסגרות ומקימה קישור ללא שגיאות בין שני מחשבים.
7. **פיסית** (Physical). מגדירה את שיטת החיבור הפיסי בין המחשבים.

פרויקט 802 של IEEE מחלק את שכבת קישור הנתונים של OSI לשתי תת-שכבות:

- **בקרת קישור לוגי** (Logical Link Control). מחזיקה את הקשר בין שני מחשבים.
- **בקרת גישה לתווך** (Media Access Control). קובעת איזה מחשב ברשת יכול להעביר נתונים בכל רגע נתון.

פרויקט 802 של IEEE גם מגדיר מספר קטגוריות המתייחסות הן לתת-השכבה בקרת גישה לתווך והן לשכבה הפיסית. הקטגוריות החשובות ביותר לזכור הן:

- 802.3 Carrier-Sense Multiple Access with Collision Detection (Ethernet)
- 802.4 Token-Bus LAN
- 802.5 Token-Ring LAN

3

רשתות מקומיות - LAN

כאשר תתחיל לתכנן את הרשת, אחת ההחלטות הראשונות שלך תהיה בדבר הפרישה הפיסית, או הטופולוגיה של הרשת. בחירה והחלטה זו עשויה להיות תלויה במספר גורמים הכוללים עלות, ציוד קיים, ארכיטקטורה ומערכות הפעלה.

בפרק זה תלמד אודות הטופולוגיות השונות וכיצד לבחור את זו המתאימה למצב שלך. עד לסוף הלימוד בפרק זה תדע כיצד:

- ✯ לתאר את הטופולוגיות אפיק (bus), כוכב (star) וטבעת (ring).
- ✯ להבין רשתות המשלבות רכיבים מטופולוגיות שונות.
- ✯ לבחור את הטופולוגיה המתאימה למצב נתון.

מהי טופולוגיה?

המונח **טופולוגיה** (topology) מתאר את הפרישה הפיסית של מחשבים, כבלים, נתבים וציוד אחר ברשת. אם תשרטט את רשת המחשבים המשרדית שלך על דף נייר, כולל שרטוט החיבורים בין מחשבים, יהיה זה שרטוט הטופולוגיה של הרשת. הטופולוגיה היא בפשטות הפרישה הפיסית של הרשת.

קיימים שלושה סוגים עיקריים של רשתות: רשת אפיק (Bus), רשת כוכב (Star) ורשת טבעת (Ring). בהמשך נעסוק בכל אחת מהן בהרחבה.

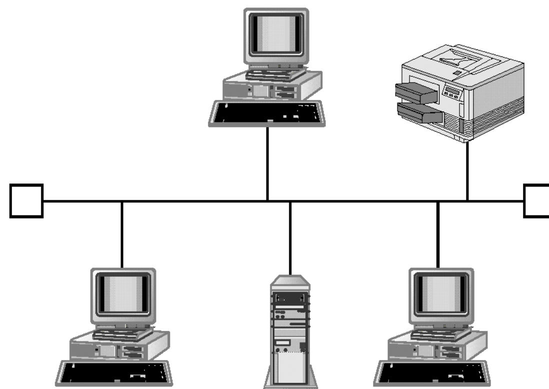
טופולוגיית אפיק (Bus)

טופולוגיית אפיק - רשת קטנה, פשוטה, עלות נמוכה וקלה להתקנה, אך קשה לארגון מחדש. נתאר מצב של חברה קטנה, שבה לכל אחד יש משרד קטן המחובר למסדרון ארוך. אין במשרד מרכזנית, ועל כולם להשתתף באחריות של מענה לטלפונים. בנוסף, אין כל מערכת אינטרקום. כאשר נכנסת שיחה שאינה מיועדת לך, עליך להעביר אותה תחילה למצב המתנה, ואז לקרוא בקול במסדרון את שם האדם שאליו מיועדת השיחה ואת מספר קו הטלפון שבו התקבלה. האדם שאליו מיועדת השיחה ירים את שפופרת הטלפון ויתקשר בקו הנכון כדי לענות לשיחה. בנוסף לסיוע במענה לטלפון, אתה גם מקשיב כל העת לשמוע אם שמך נקרא, דבר שיציין קבלת שיחה עבורך.

בעוד שמערכת זו **פשוטה**, היא אינה נקיה מבעיות. כולם צריכים להאזין כל הזמן. עם כניסת שיחות רבות יותר, רמת הרעש במסדרון עולה. אם שני אנשים ינסו לקרוא בקול בו-זמנית, לא תוכל לקבוע מי אמר מה; אנשים צריכים לקרוא בקול לפי תור. עם הוספת אנשים והארכת המסדרון, קשה יותר לשמוע מה אנשים אומרים בקצה השני של המסדרון.

זהו למעשה אופן פעולתה של רשת מחשבים המשתמשת בטופולוגיית **אפיק** (bus), הנקראת לפעמים **אפיק ליניארי** (linear bus).

כל המחשבים מחוברים **לאפיק שידרה** (backbone), או **כבל ראשי** (trunk). כפי שניתן לראות בתרשים 3.1, אפיק שידרה זה מקשר בין כל המחשבים.



תרשים 3.1: *בטופולוגיית אפיק כל המחשבים מחוברים בשורה*

כאשר מחשב רוצה להתקשר, הוא שולח אות בכבל. בדיוק כפי שהקול שלך נשמע בכל הכיוונים במסדרון, גם האות של המחשב מתקדם בשני הכיוונים בכבל. כל שאר המחשבים מקבלים את האות וקובעים אם הפנייה, או מנת הנתונים מיועדת אליהם. מחשב היעד מקבל את המידע ומתחיל בעיבוד הנתונים, אך כל שאר המחשבים מתעלמים מהאות. טופולוגיית אפיק היא טופולוגיה **פסיבית** (passive) מכיון שהמחשבים (או ה**צמתים** - nodes) ברשת רק מקשיבים ומקבלים את האות. הם אינם מגבירים את האות או משנים אותו בדרך כלשהי.

בתרחיש המסדרון, אם שני אנשים יקראו בשמות בו-זמנית, האוזניים שלנו מתוחכמות מספיק כך שנוכל לקבוע מה כל אחד אמר. מחשבים אינם כה חכמים, ולכן רק מחשב אחד יכול לשדר אות ברשת בכל רגע נתון. אם שני מחשבים משדרים מנות נתונים באותה עת, התנגשות (collision) מנות הנתונים גורמת לאות להיות בלתי ניתן לשימוש.

הבדל נוסף ביחס לעולם הפיסי הוא משך האות. אם אתה קורא בקול במסדרון, הקול שלך דועך מהר מאוד לאחר סיום דבריך.

בכבלי נחושת, אות חשמלי יכול להימשך זמן רב וכאשר הוא יגיע לקצה הכבל הוא יוחזר לכיוון השני. האות החוזר ימנע ממחשבים אחרים לשדר, ולכן חייב להיות בקצה הכבל שמשתמשים בו ברשת אפיק התקן מיוחד ל"בלימת" התופעה. התקן אלקטרוני זה הוא **נגד סיום** (terminator) שנמצא בכל אחד משני קצוות הכבל, כדי לספוג את האות ולמנוע ממנו לחזור. אם לא מותקנים נגדי סיום מתאימים ברשת אפיק, לא תוכל להתבצע תקשורת כלשהי ברשת. תרשים 3.2 מציג דוגמה של נגד סיום.

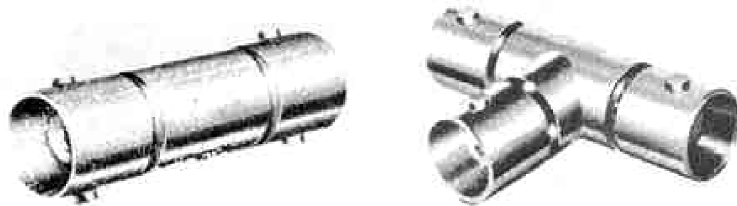


תרשים 3.2: *ברשת אפיק נדרש* ***נגד סיום*** *בקצוות הכבל כדי לספוג את האות*

היתרון הגדול ביותר של רשתות אפיק הוא הפשטות של הפרישה הפיסית. בעת שימוש בכבל דק (Thinnet), לא דרושה כל חומרה נוספת מעבר לכבלי הרשת וכרטיסי ממשק רשת. כבל Thinnet גמיש מאוד, זול וקל להתקנה. ניתן להקים רשת אפיק בין מחשבים בפרק זמן של דקות אחדות. בנוסף, רשת אפיק ניתנת להרחבה בקלות בעזרת **מחבר קנה** (barrel connector), כפי שתוכל לראות בתרשים 3.3.

רשתות אפיק המשתמשות בתווך אחר כגון כבל עבה (Thicknet) פשוטות גם הן להבנה, אולם דורשות מעט יותר עבודת התקנה.

לרשתות אפיק יש גם חסרונות. כפי שהוזכר קודם, אם כבל הרשת אינו מחובר לנגד סיום מתאים, כל התקשורת תופסק. התקשורת תופסק גם אם יש נתק במקום כלשהו בכבל. הדבר דומה לשרשרת של נורות חג, שבה נורה פגומה אחת גורמת לניתוק שאר הנורות. אם משתמש מזיז את המחשב שלו ומנתק בטעות את כבל הרשת, כל התעבורה ברשת תיפסק עד לחיבור מחדש של הכבל. מסיבה זו, כשל ברשת אפיק עלול להיות קשה מאוד לאיתור, בדיוק כמו מציאת אותה נורה **אחת** בשרשרת נורות החג. לאיתור התקלה ייתכן שתצטרך לבדוק כל אחד מחיבורי הרשת, מכיוון שהמעגל חייב להיות שלם בין כל המחשבים כתנאי לקיום התקשורת.



תרשים 3.3: *ניתן להרחיב רשת אפיק על ידי שימוש במחבר קנה (BNC barrel connector)*

חיסרון נוסף לרשת אפיק הוא מספר המחשבים שניתן לחבר לרשת. עם הוספת מחשבים, התעבורה בכבל גוברת. כל אות שנשלח חייב להיקרא על ידי כל המחשבים האחרים. בנוסף, בכל פעם שמחשב אחד שולח אות הוא מונע מהמחשבים האחרים לשלוח אותות. אם מחשב אחד מפריע לאחר, שני המחשבים שהתנגשו צריכים לנסות לשדר מחדש את האות שלהם. עם עליית התעבורה ברשת, הביצועים פוחתים.

תצורה מחדש (reconfiguring) של רשתות אפיק עלולה אף היא להיות בעייתית. יש לנתק את כבל הרשת בצומת כלשהו כדי שניתן יהיה להוסיף קטע כבל נוסף. בעת ניתוק הכבל כל התעבורה ברשת תופסק.

לסיום, האות ברשת אפיק מוגבל למרחק מסוים. אם המסדרון במשרד הדמיוני שלנו יוארך פי כמה, בסופו של דבר נגיע לנקודה שבה הקול של אדם מסוים לא יגיע מקצה אחד של המסדרון לקצהו האחר. באופן דומה, האות בכבל מוגבל למרחק מסוים, לפני שאיכות האות תידרדר לנקודה שבה האות אינו ניתן לשימוש. ניתן להאריך את טווח החיים של האות על ידי הוספת **מגבר** (repeater), המגביר את האות לפני העברתו הלאה, אולם גם הארכות אלו נתקלות במגבלות פיסיות. לדוגמה, ברשת אפיק Ethernet המשתמשת בכבל Thinnet, כל **מקטע** (segment) ברשת לא יכול לעלות על 185 מטרים (607 feet). ניתן להשתמש במגברים להגברת האות, אולם האורך הכולל של הרשת לא יכול לעלות על 925 מטרים (3,035 feet).



רעיון מפתח

בטופולוגיית אפיק (bus topology), כל מחשב מחובר ישירות לכבל הרשת הראשי בקו יחיד.

יתרונות טופולוגיית אפיק

לרשת המבוססת על טופולוגיית אפיק יש יתרונות רבים, וביניהם:

- ✯ הכבלים והחומרה שמשתמשים בהם זולים מאוד.
- ✯ ההתקנה יכולה להיות קלה ומהירה.
- ✯ הטופולוגיה קלה להבנה (הכבל עובר ממחשב אחד לאחר - האם יש פשוט מזה?).
- ✯ רשת אפיק ניתנת להרחבה בקלות (בקלות רבה כאשר יש להוסיף מחשב בודד בקצה הקו, ובקלות כאשר יש להוסיף מספר מחשבים באמצע הרשת).

חסרונות טופולוגיית אפיק

בעוד שרשתות אפיק קלות להתקנה והגדרה, הן סובלות מהחסרונות האלה:

- ✯ איתור תקלות עלול להיות בעייתי. מכיון שנתק ברשת **במקום כלשהו** עלול להפיל את כל הרשת, ייתכן שתצטרך לבדוק כל אחד מהחיבורים עד למציאת התקלה.
- ✯ עליה בתעבורת הרשת עלולה להקטין במידה משמעותית את ביצועיה.
- ✯ האורך הפיסי הכולל של הרשת מוגבל.
- ✯ הגדרה מחדש של הרשת (הוספת עמדות ו/או שינוי מיקומן) דורשת ניתוק פיסי.

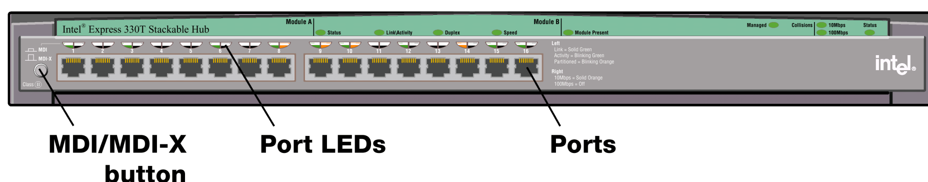
טופולוגיית כוכב (Star)

טופולוגיית כוכב (Star) - רשת קטנה, עלות נמוכה (ברשת גדולה העלות מתרחבת), התקנה קלה וכן הארגון מחדש.

נחזור אל החברה הדמיונית שלנו, שבה נוספו עובדים והיא עברה למשרד באתר חדש. כעת כל העובדים נמצאים סביב חדר מרכזי, אולם עדיין אין ברשותם אינטרקום. כאשר אחד העובדים מקבל שיחה, הוא קורא בקול לחדר המרכזי. כמו קודם, כולם חייבים להקשיב כל הזמן, אולם כעת כולם ממוקמים קרוב יותר זה לזה. בנוסף, ההנהלה תכננה מראש והשאירה משרדים ריקים רבים כהכנה להרחבה בעתיד.

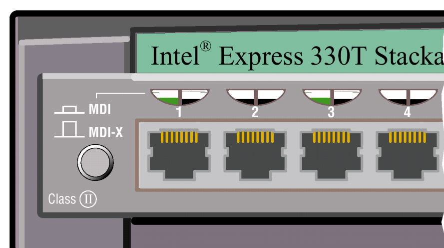
רשתות מחשבים המשתמשות **בטופולוגיית כוכב** (star topology) פועלות בצורה דומה למדי. כפי שמוצג בתרשים 3.6, כל המחשבים ברשת מחוברים ל**רכזת** (hub) המרכזית. כאשר מחשב שולח אות, הוא עובר לרכזת וממנה הוא מועבר לכל המחשבים המחוברים לרכזת.

רכזת, כמו זו שבתרשים 3.4, מכילה 16 כניסות (Ports). מעל כל כניסה יש נורית חיווי (Port LED) לציון מהירות העבודה של החיבור.



תרשים 3.4: *רכזת 16ports*

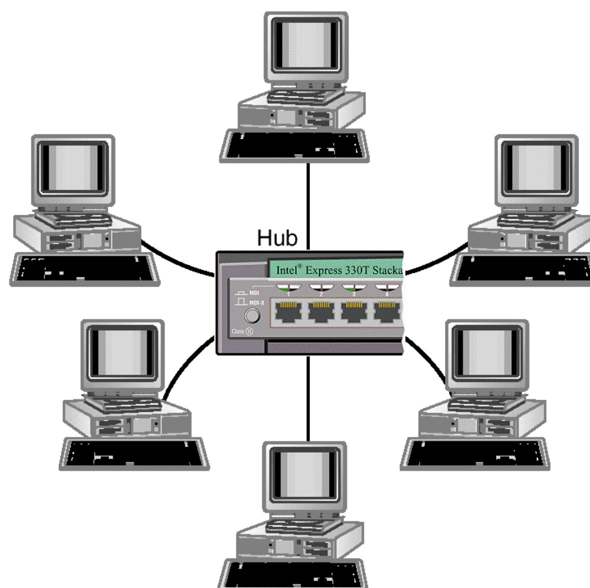
כך נראה Port מקרוב, תרשים 3.5. את החיבור הפיסי נלמד בפרק הבא.



תרשים 3.5: *מבט מקרוב על רכזת*

מקובל להשתמש בשני סוגי רכזות: **פסיבית** (passive) ו**אקטיבית** (active). ברשתות המשתמשות ב**רַכֶּזֶת** פסיבית, האות מועבר ללא שינוי לכל המחשבים האחרים. רכזות פסיביות משמשות בעיקר ברשתות קטנות, מכיון שהן סומכות רק על כוח המחשבים להעברת האות. אם המחשבים נמצאים במרחק זה מזה, את הנתונים ממחשב אחד עלול **להיחלש** (degrade) לפני שיגיע לאחרים (הדבר דומה לטופולוגיית אפיק, שבה אותות יכולים לעבור רק מרחק מוגבל לפני שאיכות האות מתחילה להתדרדר).

מצד שני, רכזות אקטיביות, הנקראות לעיתים **מגברים מרובי יציאות** (multiport repeaters), משתמשות במתח חשמלי להגברת אות הנתונים, ומאפשרות לאות לעבור מרחק רב יותר באיכות גבוהה יותר. רכזות אקטיביות מתאימות יותר לרשתות גדולות, שבהן עשוי האות לעבור מרחקים גדולים.



תרשים 3.6: *רשת בטופולוגיית כוכב משתמשת ברכזת (hub) לחיבור כל המחשבים*

יש דמיון מסוים בין טופולוגיית כוכב לטופולוגיית אפיק בהעברת הנתונים. בשתיהן רק מחשב אחד יכול להעביר אות נתונים בכל רגע נתון. בנוסף, כל מחשב מקבל את כל מנות הנתונים וחייב לבדוק את כתובת היעד של כל מנה. כאשר הוא מזהה מנה המיועדת אליו, הוא מעביר אותה לשכבות הגבוהות יותר של מודל OSI. המחשב מתעלם מכל המנות המיועדות למחשבים אחרים.

אולם, שלא כמו בטופולוגיית אפיק, נתק בחיבור רשת אחד **לא** יפיל את כל הרשת. המחשב עם הכבל המנותק לא יוכל להתקשר עם השאר, אולם התקשורת בין שאר המחשבים תמשיך ללא הפרעה. מסיבה זו, בדרך כלל קל לאתר תקלות ברשתות כוכב. מתוך הבנת הטופולוגיה גם ברור שאם הרכזת תתקלקל, כל הרשת תיפול. אולם מלבד זאת, רשתות כוכב נחשבות אמינות.

קל ופשוט לשנות תצורה של רשתות כוכב. כדי להוסיף מחשב, יש לחבר כבל חדש בין הרכזת לבין המחשב החדש. אם ברצונך להעביר כבל מכניסה אחת ברכזת לאחרת, ניתן לעשות זאת בלי להפריע לשאר חלקי הרשת. ניתן לנתק מחשב בכל עת על ידי ניתוק התקע שלו. אם בסופו של דבר אוזל המקום ברכזת, ניתן לרכוש רכזת גדולה יותר ולהעביר אליה את הכבלים בקלות רבה.

ברשת קטנה, טופולוגיית כוכב יכולה להיות זולה יחסית. מכיון שלרוב נעשה שימוש בכבל **זוג שזור לא מסוכך - UTP** (unshielded twisted pair) הזול (דומה מאוד לחוט טלפון), הרכיב היקר ביותר במערכת הוא הרכזת. אולם עם הרחבת רשת כוכב, עלות הכבלים עלולה לגדול במהירות. בעוד שכבל בטופולוגיית אפיק עובר ממחשב אחד לבא אחריו, הכבלים בכוכב מחוברים מכל מחשב אל הרכזת. אם יש מספר מחשבים

שנמצאים במרחק רב מהרכזת, תצטרך למתוח כבל נפרד עבור כל מחשב מהרכזת ואליו.

הצורך בכבלים נפרדים עלול להציב גם מגבלת מרחק. ככלל, מרבית סוגי תווך הרשת המשתמשים ברשתות כוכב מגבילים את מיקום המחשבים למרחק שאינו עולה על 100 מטרים (328 feet) מהרכזת.



רעיון מפתח

בטופולוגיית כוכב (star topology), כל המחשבים מחוברים באמצעות רַכֶּזֶת (hub). כבל נפרד עובר מכל מחשב בחזרה לרכזת.

יתרונות טופולוגיית כוכב

לרשת המבוססת על טופולוגיית כוכב יש יתרונות רבים:

- כשל במחשב יחיד לא יפריע לתקשורת בין מחשבים אחרים.
- איתור תקלות בקלות יחסית, מכיון שהחיבורים הם בין הרכזת למחשבים יחידים.
- קל להוסיף מחשבים לרשת ולהגדיר מחדש חיבורים.

חסרונות טופולוגיית כוכב

חסרונות טופולוגיית כוכב כוללים:

- כבלים עלולים להיות יקרים בגלל הצורך בכבל נפרד בין הרכזת לכל אחד מהמחשבים.
- כשל ברכזת יפסיק את כל התקשורת ברשת.
- הגבלת מרחק המחשבים מהרכזת, בגלל הצורך בכבלים נפרדים לכל אחד.

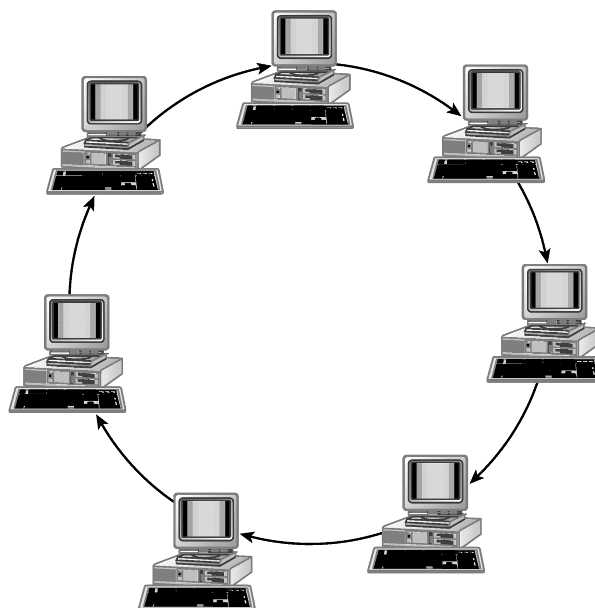
טופולוגיית טבעת (Ring)

טופולוגיית טבעת - גישה סדרתית ושווה לרשת, פיסית דומה לרשת אפיק מעגלית. נחזור לתרחיש המשרד. קריאה בקול למסדרון או לחדר מרכזי לצורך העברת הודעות הפכה למעייפת ולא יעילה. בנוסף, הקולות החזקים ביותר נטו לגבור על אלה עם הקולות החלשים יותר.

כעת החברה שלך החליטה להעסיק שליח שיעבור בכל המשרדים ויבדוק אם יש הודעות. שליח זה מסתובב במשרד מקבל ומעביר הודעות. בכל פעם שאתה מקבל הודעה עבור מישהו, אתה רושם אותה על פתק ומניח במקום שהשליח יאסוף אותה משם. השליח אוסף את ההודעה, מספק אותה לאדם המתאים, בודק שוב אם יש הודעות להעברה, וממשיך הלאה למשרד הבא. בדרך זו, ההודעות עוברות מעובד לעובד ללא צעקות. בנוסף, מכיון שלא ניתן להעביר הודעה עד שהשליח מגיע לאסוף

אותה, אף אחד אינו יכול להפריע לאספקת הודעה של מישהו אחר. ולסיום, מכיון שהשליח עוצר בכל משרד, כולם יכולים להיות בטוחים שתהיה להם הזדמנות לשלוח הודעה.

למרות ששיטה זו אולי אינה קיימת בעולם הפיסי (אלא רק בתיאוריה), זהו אופן הפעולה של רשתות המבוססות על **טופולוגיית טבעת** (ring topology). כפי שניתן לראות בתרשים 3.7, כל המחשבים ברשת מחוברים במעגל יחיד של כבל ללא קצוות והאות עובר בכיוון אחד בטבעת. ארכיטקטורות מסוימות המממשות טופולוגיה זו, כגון FDDI, הטבעת עשויה לכלול כבל מעגלי יחיד, ובארכיטקטורות אחרות כדוגמת **טבעת אסימון** (Token Ring) נעשה שילוב של כוכב וטבעת, כפי שנלמד בהמשך פרק זה.



תרשים 3.7: *טופולוגיית טבעת מחברת את כל המחשבים בטבעת (ומכאן השם). רשת זו קיימת בתיאוריה בלבד.*

הטבעת היא דוגמה לטופולוגיה **אקטיבית**, במובן שכל מחשב לא רק מקבל את הנתונים, אלא עושה יותר מכך. לאחר קבלת המנה, כל מחשב מגביר את האות הנקלט ושולח אותו אל המחשב הבא. כתוצאה מכך, רשתות טבעת אינן סובלות מאותה דעיכת אות המתרחשת ברשתות אפיק וכוכב, ככל שהאות עובר מרחק רב יותר.



רעיון מפתח

בטופולוגיית טבעת (ring topology), כל המחשבים מחוברים במעגל.

טבעות רבות מיישמות מערכת של **העברת אסימון** (token passing), שבדומה לשליח בתרחיש המשרד שלנו, מבטיחה שכל מחשב יקבל הזדמנות שווה לתקשורת ברשת.



רעיון מפתח

אסימון (token) הוא מנת נתונים קטנה המועברת ברציפות בין המחשבים שבטבעת. כל מחשב יכול לשדר הודעה רק כאשר האסימון נמצא אצלו.

יתרונות טופולוגיית טבעת

יתרונות טופולוגיית טבעת כוללים:

- המנגנון לגישה הוגנת (העברת אסימון) מספק הזדמנויות שוות לכל המחשבים לתקשר.
- התקנה פשוטה.
- מכיון שהאות מחודש בכל מחשב, אין דעיכת אות בדומה לרשתות אחרות.

חסרונות טופולוגיית טבעת

החסרונות כוללים:

- כמו באפיק, כשל בחיבור כלשהו עלול להפיל את כל המערכת (שים לב לכך שרשתות טבעת אחדות, כגון אלו המשתמשות בארכיטקטורת FDDI, עשויות לכלול טבעת משנית להפחתת תקלות ברשת).
- תצורה מחדש עלולה להיות מסובכת, מכיון שיש להפסיק את פעולת הרשת בעת הוספת החיבור החדש.
- המרחק עלול להיות מוגבל כתוצאה ממגבלות התווך הפיסי, חיבורי הכבלים חייבים להיסגר למעגל אחד גדול.

הכלאת טופולוגיות (Hybrid)

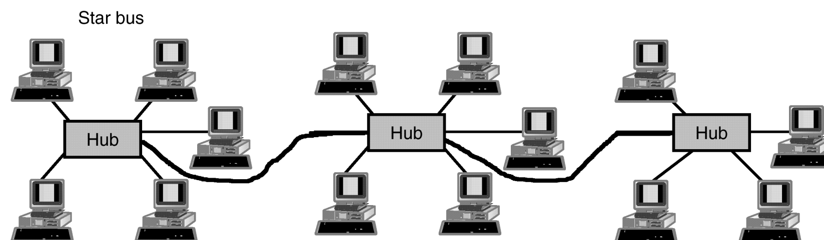
למרות שאלו הן שלוש הטופולוגיות הבסיסיות, ניתן ליצור מהן גרסאות שונות ורבות. במרבית הרשתות ניתן למצוא מרכיבים מטופולוגיות שונות. שלוש הגרסאות הנפוצות ביותר מתוארות בסעיפים שלפניך:

כוכב אפיק (Star Bus)

כוכב אפיק (star bus) - רשת גדולה, קלה להתקנה הרחבה וארגון מחדש. טופולוגיית כוכב אפיק, המתוארת בתרשים 3.8, מורכבת למעשה ממספר רשתות כוכב המחוברות על ידי רשת אפיק. ארגון יכול להפעיל תחילה רשת כוכב עם רכזת אחת. כאשר הרשת גדלה לממדים בהם רכזת אחת מלאה, ניתן להוסיף רכזת נוספת ולקשר אותה בכבל לרכזת הראשונה. עם הוספת הרכזת השלישית היא תחובר לרכזת השנייה, וכך הלאה.

ניתן גם למצוא תצורה זו בבניין משרדים רב קומתי. בכל קומה ניתן להציב רכזת (או מספר רכזות) שיחוברו זו לזו על ידי אפיק העובר מקומה לקומה.

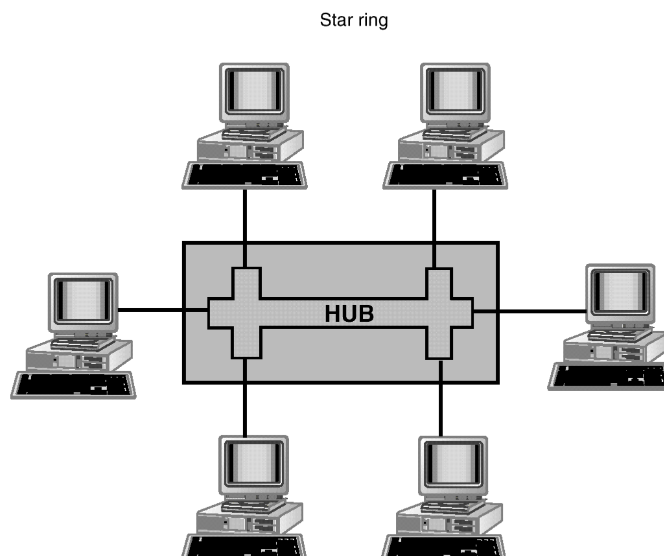
לטופולוגיית כוכב אפיק יש יתרונות של טופולוגיית כוכב, בכך שנפילת מחשב אחד לא תפיל את כל הרשת ובכך שקל לשנות את התצורה שלה. כמו בטופולוגיית כוכב, אם רכזת כושלת, כל המחשבים המחוברים לרכזת זו לא יוכלו לתקשר. בדומה לטופולוגיית אפיק, אם יש נתק בין רכזות, מחשבים יוכלו לתקשר עם מחשבים אחרים המחוברים לאותה רכזת, אולם לא עם אלה המחוברים לרכזות אחרות.



תרשים 3.8: *בטופולוגיית* ***כוכב אפיק*** *נראה מספר רכזות שמחוברות ברשת אפיק. החיבור בין הרשתות (בין הרכזות) נעשה על ידי כבל מיוחד.*

כוכב טבעת (Star Ring)

כוכב טבעת - רשת כוכב עם גישה שווה לרשת. טופולוגיית טבעת עלולה להיות קשה למימוש, ולכן טופולוגיית **כוכב טבעת**, או **כוכב מחווט לטבעת** (star-wired ring) הינה תחליף מתאים. היא מספקת מנגנון קל יותר להשגת טבעת (ראה תרשים 3.9), כי הכבלים מחוברים פיסית כמו בטופולוגיית כוכב. עם זאת, בתוך הרכזת התקעים מחוברים במבנה טבעת. רוב רשתות טבעת אסימון ממומשות כך.



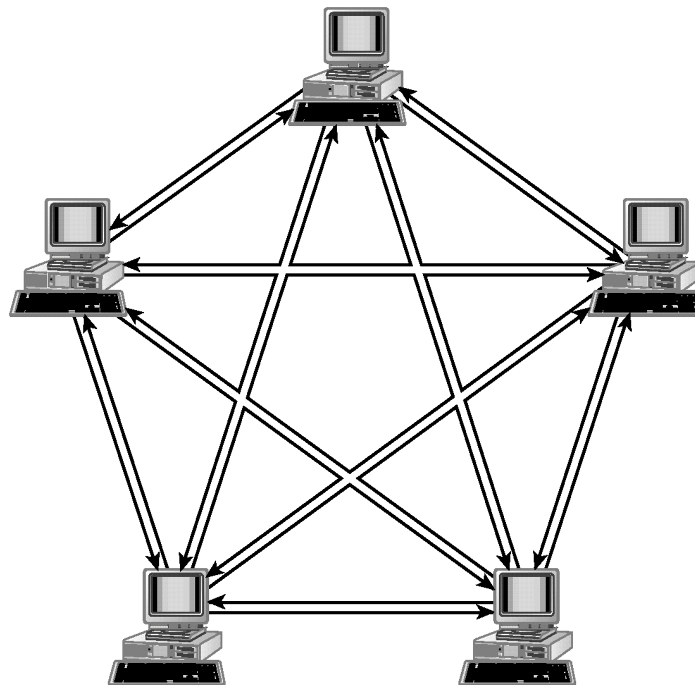
תרשים 3.9: *בטופולוגיית כוכב טבעת המחשבים מחוברים בכוכב פיסי, אולם הרכזת מחווטת באופן שיוצר רשת טבעת*

לטופולוגיה זו יש יתרונות של רשת כוכב בתוספת היתרונות של גישה שוויונית של טופולוגיית טבעת. טבעת כוכב סובלת מחסרונות דומים לטופולוגיית כוכב, כולל מגבלת אורך פיסי של כבל וכשל ברשת כתוצאה מכשל ברכזת.

סריג (Mesh)

סריג (Mesh) - רשת מסובכת, עלות גבוהה, ארגון מחדש קשה אך נהנית מהיציבות הגבוהה ביותר. אם תעבוד עם שלושה אנשים ותשבו כולכם סביב שולחן יחיד, התקשורת תהיה פשוטה מאוד. תוכל להסתכל ישירות אל האדם שאיתו אתה רוצה לתקשר ולהתחיל לדבר. לא יהיה כל צורך להמתין שכל האחרים יפסיקו לדבר ביניהם, או להמתין לשליח. לכל אחד מכם תהיה גישה ישירה לכל אחד אחר.

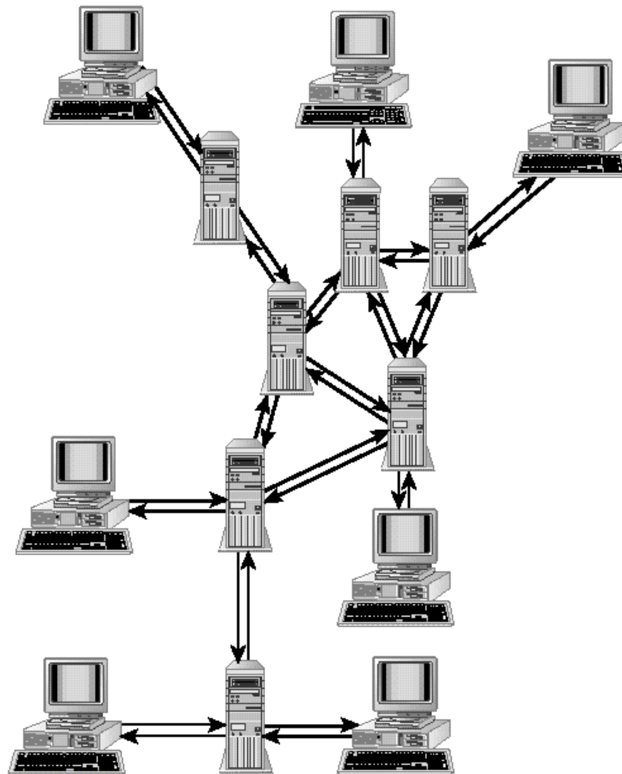
רשת סריג (mesh network) אמיתית היא כזו שבה לכל מחשב יש חיבור לכל מחשב אחר ברשת כפי שמתואר בתרשים 3.10. היתרון בכך הוא שניתן להיות כמעט בטוח שהודעות יעברו תמיד. אפילו אם הקשר הישיר שלך עם מחשב אחר כשל, תוכל להעביר את ההודעה מהמחשב שלך למחשב אחר, ומשם ליעד המקורי. על רשתות סריג נאמר כי הן עמידות מאוד בפני תקלות (highly fault-tolerant).



תרשים 3.10: *ברשת סריג אמיתית לכל מחשב יש חיבור לכל מחשב אחר*

רשתות סריג אינן מעשיות ברוב המצבים. העלות של חיבורים מרובים הופכת במהירות למרתיעה. בנוסף, התקנה ותצורה מחדש של רשתות סריג עלולה להפוך לסיוט.

ניתן למצוא רשתות סריג היברידיות (hybrid), כאשר לחלק מהקשרים יש חיבורים יתירים. לדוגמה, חברה יכולה להשתמש במספר קשרים על פני רשת מרחבית המקשרת בין משרדים, כדי שאם קשר אחד אינו פועל, המשרדים יוכלו בכל זאת לתקשר זה עם זה. חברה המבצעת עבודה רבה על פני האינטרנט עשויה להעדיף מספר קשרים אל ספק שירותי האינטרנט שלה, כדי שהגישה לאינטרנט תהיה זמינה בכל עת. רשתות היברידיות כגון אלו (ראה תרשים 3.11) מספקות מידה מסוימת של עמידות בפני תקלות, אך ללא העלות העצומה של סריג אמיתי.



תרשים 3.11: *רשת סריג היברידית מכילה חיבורים יתירים בין חלק מהצמתים ברשת*

בחירת הטופולוגיה המתאימה

הטופולוגיה שבה תשתמש תהיה תלויה במספר גורמים, כולל עלות, מרחק, פרק זמן מוקצב להתקנה, וסביבה פיסית. הגורמים שיש להתחשב בהם הם:

- אם אתה מתקין רשת קטנה בחדר או במשרד ומחפש מנגנון זול לעשות זאת, רשת אפיק, או רשת כוכב יספקו ככל הנראה את הפתרון הטוב ביותר.
- אם אתה יודע שבעתיד תוסיף למערכת או תשנה את תצורתה, טופולוגיית כוכב היא ללא ספק הקלה ביותר לתצורה מחדש.

- ✯ אם יש לך מספר גדול של משתמשים באזור מוגבל יחסית, רשת מסוג כוכב אפיק עשויה לספק את כל יכולת ההרחבה הדרושה לך.
- ✯ אם אתה מחפש מנגנון שיספק גישה שווה לתווך הרשת, ואפילו בתנאים של תעבורת רשת גבוהה, בחר בטופולוגיית טבעת.
- ✯ אם אתה רוצה ברשת בעלת עמידות גבוהה במיוחד בפני תקלות, בחר בטופולוגיית סריג.

סיכום

טופולוגיית רשת מתארת את הפרישה הפיסית של רשת מחשבים. הסוגים העיקריים של טופולוגיות כוללים **אפיק** (bus), **כוכב** (star) ו**טבעת** (ring).

ברשת המבוססת על **טופולוגיית אפיק** (bus technology), כל המחשבים מחוברים בקו אחד. רשת אפיק זולה מאוד וקלה מאוד להתקנה. החיסרון הבולט שלה הוא שנתק כלשהו בכבל עלול לגרום לנפילת הרשת כולה.

טופולוגיית כוכב (star topology) משתמשת בהתקן הנקרא **רכזת** (hub) כנקודת איסוף מרכזית לכל חיבורי הרשת. כבל עובר ישירות מכל מחשב אל הרכזת המרכזית הזו. כך קל לאתר תקלות ולשנות תצורה של הרשת. כל מחשב הינו עצמאי, ולכן תקלה בחיבור רשת אחד לא תסכן את כלל הרשת. החסרונות של רשתות כוכב כוללים עלות גבוהה כתוצאה ממספר הכבלים הדרושים וסכנה שכשל ברכזת יפיל את כלל הרשת.

מחשבים ב**טופולוגיית טבעת** (ring topology) אמיתית מחוברים כולם בטבעת כבל יחידה. מרבית הטבעות משתמשות בסוג כלשהו של **העברת אסימון** (token passing), כדי לספק לכל מחשב גישה שווה לרשת. כמו ברשתות אפיק, גם כאן כשל במחשב אחד עלול להפיל את הרשת כולה. כתוצאה מקושי במימוש פיסי של רשת טבעת, מרבים להתקין רשתות מסוג זה כרשתות **כוכב טבעת** (star-wired ring).

ניתן גם למצוא גרסאות שונות לשילוב, ובהן: רשתות **כוכב אפיק** (star bus), **כוכב טבעת** (star ring) ו**סריג** (mesh). רשתות **היברידיות** (hybrid) אלו מכילות רכיבים מטופולוגיות אחרות.

4

החיבור הפיסי

לא חשוב כיצד תתכנן את הרשת שלך, היא מסתכמת בסופו של דבר בהעברת סיביות נתונים על פני סוג כלשהו של חיבור בין מחשבים. פרק זה יתאר את סוגי התווך שבשימוש ואת השיטות שבהן נעשה שימוש בסוגי תווך אלה.

עד סוף הפרק, תוכל:

- ✯ להבין מונחים הקשורים לתווך פיסי,
- ✯ לדעת את ההבדלים בין סוגים עיקריים של כבלים,
- ✯ להבין באיזה סוג כבל להשתמש במצבים שונים.

ביצוע החיבור

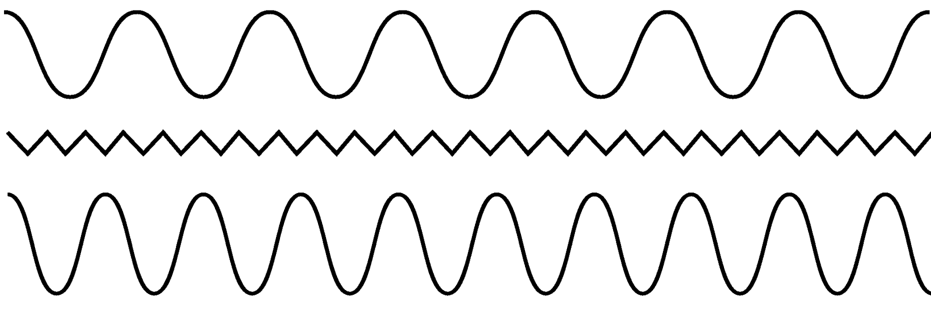
בסופו של דבר, תקשורת על פני רשת מחשבים מסתכמת בהעברה של אות על פני תווך. ברוב הרשתות העברה זו מתרחשת כאות חשמלי העובר בחוט נחושת. בחלק מהמקרים, ייעשה שימוש באור בתוך סיב אופטי. אולם הרעיון בשני המקרים הינו אחד - כיצד מיוצגים הנתונים האלקטרוניים כ**פעימות** (impulses) בכבל?

מרבית הרשתות המקומיות (LAN) משתמשות **בתמסורת פס-בסיס** (baseband transmission) דיגיטלית כאשר סיביות הנתונים 1 ו-0 מוגדרות כשינויים נבדלים בזרימת החשמל או האור. הדבר דומה לתקשורת בלילה באמצעות פנס. האור דולק או כבוי.

כפי שמוצג בתרשים 4.1, קיימים רק שני מצבים - פועל או כבוי - כל כבל התקשורת עסוק בהעברת נתונים. היתרון בשידור baseband הוא שהתקנים המחוברים זה לזה יכולים לקלוט ולשדר באותה עת.

תרשים 4.1: *בתמסורת baseband מוגדרות סיביות הנתונים על ידי שינויים נבדלים באות*

לעומת זאת, **תמסורת פס-רחב (broadband transmission)** משתמשת בתקשורת אנלוגית לחלוקת הכבל לסדרת ערוצים, כפי שמוצג בתרשים 4.2. לכל ערוץ יש תדר נפרד, וכל ההתקנים המקשיבים לתדר זה יכולים לקבל את הנתונים. טלוויזיה בכבלים משתמשת בטכנולוגיה זו להכנסת מספר רב של ערוצים לבית דרך כבל יחיד. כבל דומה לזה המשמש טלוויזיה בכבלים יכול לשמש במצבים מסוימים כדי לאפשר הן לקול והן לנתוני רשת לעבור באותו כבל פיסי וזהו היישום של אינטרנט מהיר.



תרשים 4.2: *מספר ערוצי נתונים עוברים דרך כבל יחיד בעת שימוש בתמסורת broadband*

למרות שתמסורת broadband גמישה יותר, עלות ציוד החיבור בדרך כלל גבוהה יותר. בנוסף, כל ערוץ בקו broadband יכול לשדר רק בכיוון אחד. לתקשורת דו-כיוונית (הדרושה בסביבת רשת מקומית) נדרש ערוץ נפרד לכל כיוון של תעבורה ברשת.



רעיון מפתח

תקשורת **פס בסיס** (baseband) משתמשת בטכנולוגיה דיגיטלית. טכנולוגיית **פס-רחב** (broadband) משתמשת בנתונים אנלוגיים.

ללא קשר לסוג השידור שתבחר, תוכל להשתמש בסוגי תווך פיסי (physical media) רבים. למרות שיש אלפי סוגים שונים של כבלי רשת, ניתן לחלקם לשלושה סוגים עיקריים:

- **זוג שזור** (twisted-pair),
- **קואקסיאלי** (coaxial),
- **סיב-אופטי** (fiber-optic).

לכל אחד משלושה סוגי תווך אלה יש יתרונות וחסרונות. חלקם מתאימים לרשתות מסוימות, בעוד אחרים אינם מתאימים.

לפני שנדון בסוגי התווך השונים, עליך להכיר מספר מונחים:

- **דעיכה (Attenuation)**. משלוח אותות על פני תווך דורש אנרגיה. אם אתה נוסע במכוניתך ומקשיב לתחנת רדיו, תתחיל לאבד את התחנה ככל שתתרחק ממיקום המשדר. בסופו של דבר התחנה תדעך לחלוטין. באופן דומה בעולם הרישות, דרושה אנרגיה לשידור נתונים בכבל. ככל שהאות מתקדם בכבל, הוא נחלש כאשר חלק מהאות נספג בתווך. תהליך זה, המכונה Attenuation, מציב מגבלות על האורך הפיסי של הכבל. תווך כמו חוטי נחושת דועך במהירות וניתן להשתמש בו למרחקים קצרים יחסית בלבד. לעומת זאת כבלים עשויים סיב-אופטי, כמעט ואינם סובלים מהיחלשות האות, וניתן להשתמש בהם להעברת נתונים על פני מרחקים גדולים.
- **רוחב פס (Bandwidth).** בתווך רשת, רוחב הפס של חיבור מתייחס למספר הסיביות שניתן לשלוח בכבל ברגע נתון. הוא נמדד בדרך כלל ב-Mbps (מיליון סיביות לשנייה), כאשר 1Mbps פירושו שמיליון סיביות יועברו בכל שנייה. רוב הרשתות פועלות בקצב שידור של כ- 10Mbps, אולם רשתות חדשות רבות יכולות לפעול עד 100Mbps. רשתות סיבים אופטיים הן כה מהירות, שעבורן קיים המונח Gbps (Giga-bits-per-second), או מיליארד סיביות לשנייה. קיימים חיבורי סיב-אופטי הפועלים במהירות של 2-200Gbps.
- **עכבה (Impedance).** עכבה היא התנגדות החוט לשידור אות חשמלי. ככל שהעכבה גבוהה, כך דרושה אנרגיה גבוהה יותר לשידור האות בחוט. עכבה נמדדת ביחידות של אוהם (Ohm).

* **הפרעה (Interference).** נקראת גם הפרעה אלקטרומגנטית או EMI. אם נסעת בכביש מהיר ושמעת את תחנת הרדיו שלך דועכת כאשר עברת מתחת לקווי מתח גבוה, חווית הפרעה. כאשר אות חשמלי עובר בכבל, חלק מהאנרגיה שלו נספגת בכבל עצמו וחלק ממנה מוקרנת אל מחוץ לחוט. אנרגיה מוקרנת זו, הנקראת גם **רעש** (noise), יכולה להפריע לאותות של חוטים והתקנים אחרים. באופן דומה, האות מהתקנים קרובים אחרים יכול להפריע לאות החשמלי שבחוט. הפרעות רבות עלולות לגרום להתדרדרות האות עד לנקודה שלא ניתן יותר להכירו.
* סוג מסוים של הפרעה המכונה crosstalk מתרחש כאשר שני חוטים מונחים זה לצד זה בתוך כבל. במקרה זה, הרעש מכל קו עלול להפריע לאות בקו השני.



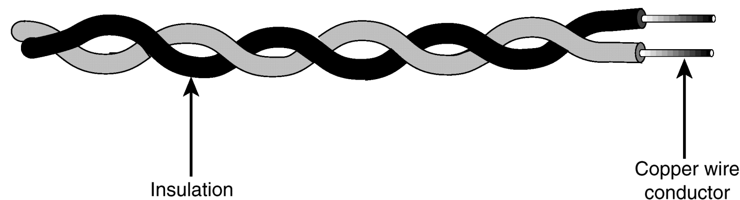
הערה: הפרעות עלולות גם לעורר בעיה של אבטחת מידע בארגון. האנרגיה המוקרנת מכבל יכולה לא רק להפריע להתקנים אחרים, אלא שהיא ניתנת גם לקליטה על ידי מישהו המנסה "לצותת" לתשדורות שלך. אם האבטחה חשובה לך, תווך סיבים אופטיים אשר אינו רגיש ל- EMI עשוי להיות הבחירה הטובה ביותר עבור הרשת שלך.

* **חללי אוורור (Plenum)**. בבנייני משרדים מודרניים רבים, יש תקרה כפולה שבחלל שלה עוברים מרבית הכבלים (חשמל, טלפון, רשת) החיוניים לעבודת המשרד. חלל זה, הנקרא plenum, משמש לרוב גם למיחזור האוויר בבניין. במקרה של דליקה, סוג הכבל שנמצא בחלל אוויר זה הוא בעל חשיבות קריטית. למרבית הכבלים יש שכבה חיצונית גמישה וזולה של PVC (polyvinyl chloride). הבעיה עם PVC היא שבעת שריפה הוא משחרר גזים רעילים מאוד, העלולים להתפשט בקלות בבניין דרך חללי האוורור האלה. לכן, כמעט כל נוהלי בטיחות אש דורשים שימוש בכבלים מיוחדים להתקנה בחללי האוויר שבתקרות כפולות ובמרחבים אחרים הקשורים לסחרור אוויר. כבלי plenum אלה עמידים יותר בשריפה ואינם משחררים כמות כה רבה של אדים, אולם חסרונם בכך שהם יקרים יותר.
* **סיכוך (Shielding).** להפחתת ההפרעות לאות חשמלי בכבל, דרוש סוג כלשהו של סיכוך שעוטף את הכבל המוליך. הוא עשוי להיות בצורת שכבה מתכתית דקה (foil) או רשת פלדה ארוגה (woven steel mesh). למרות שסיכוך מפחית את ההפרעות בכבל, הוא מגביר את עלות הכבל ומקטין את הגמישות, ולכן מקשה על ההתקנה.

כעת, לאחר שלמדת מספר מונחים בנושא כבלים, תוכל להמשיך בדיון סוגי התווך ברשת.

כבל זוג שזור (TP - Twisted Pair)

האם קנית פעם כבל מאריך לטלפון? אם כן, השתמשת ככל הנראה בכבל זוג שזור. רוב הרשתות כיום פועלות על כבלים הדומים לקווי הטלפון הרגילים שלנו.



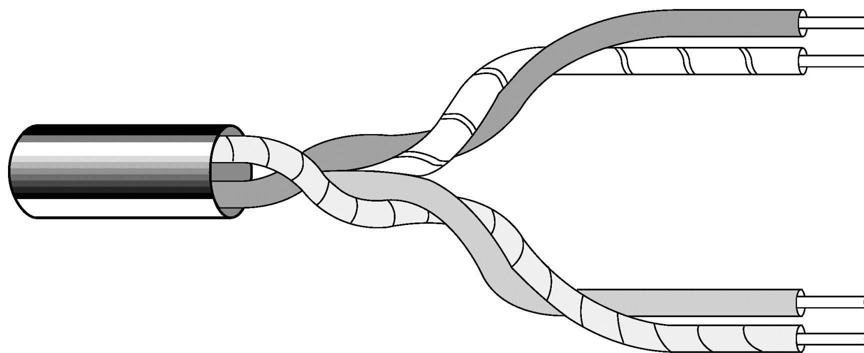
תרשים 4.3: *כבל זוג שזור מכיל שני חוטי נחושת המלופפים זה סביב זה*

בתוך כבל זוג שזור תמצא מספר רב של זוגות חוטי נחושת, כפי שניתן לראות בתרשים 4.3. כל חוט עטוף בבידוד הפלסטי שלו בצבע מסוים. אם החוטים היו מונחים זה לצד זה, ה-**crosstalk** בין החוטים היה מפריע לאות עד כדי כך שהחוטים היו חסרי תועלת. במקום זאת, החוטים מלופפים זה סביב זה. פעולת שזירה זו מבטלת את ההפרעות בין החוטים. ניתן למצוא שני סוגים של כבלי זוג שזור: מסוכך ולא-מסוכך.

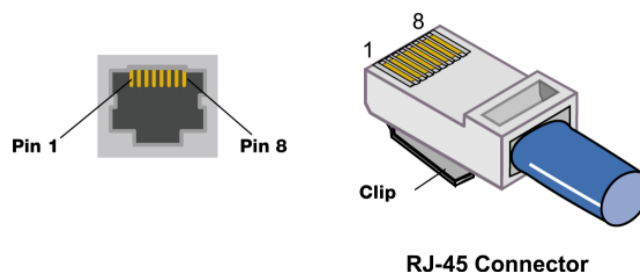
זוג שזור לא-מסוכך
(UTP - Unshielded Twisted Pair)

זוג שזור לא-מסוכך, המוכר כ-**UTP** (Unshielded Twisted Pair), הוא ככל הנראה תווך הרשת הנפוץ ביותר בסביבת המשרד כיום. כבל מסוג UTP אינו יקר, גמיש מאוד, וקל מאוד להתקנה ותחזוקה. מכיון ש-UTP משמש גם להתקנות טלפונים, הציוד המוגדר לשימוש עם כבלי זוגות שזורים לא-מסוככים כבר קיים בשפע.

כפי שניתן לראות בתרשים 4.4, זוג שזור לא-מסוכך המשמש למערכות טלפון ביתיות מקובלות מכיל ארבעה חוטים (שני זוגות), ויש לו חיבורים בשני קצותיו באמצעות מחברי RJ-11. בדרך כלל, סוג זה של UTP אינו משמש ברשתות מחשבים. במקום זאת, רוב הרשתות משתמשות ב-UTP עם שמונה חוטים (ארבעה זוגות) ומחבר מעט גדול יותר RJ-45 בכל קצה, תרשים 4.5.



תרשים 4.4: *כבל זוג שזור לא-מסוכך יכול להכיל שני זוגות של חוטי נחושת שזורים*



תרשים 4.5: *מחבר RJ-45 ושקע החיבור שלו לקיר/ללוח חיבורים ו/או לרכזת.*

כבלי UTP מחוברים בדרך כלל ישירות מכרטיס ממשק הרשת במחשב לשקע בקיר. מכאן, כבלי UTP מחוברים ל**לוח חיבורים** (patch panel), שבו **חוטי חיבור** (patch cords) נוספים מחברים את האות ל**רכזת** (hub), או להתקן דומה אחר.

כבלי UTP מחולקים לחמש קטגוריות לפי תקן שנכתב על ידי **TIA/EIA** (Telecommunications Industries Association ו-Electronic Industries Association). תקן "Commercial Building Wiring Standard 568" של EIA/TIA מפרט מידע כגון מהירות העברת הנתונים ומספר הליפופים ברגל. טבלה 4.1 מפרטת את הקטגוריות של כבלי UTP נפוצים.



רעיון מפתח

זכור ש- Category 3 UTP הוא המינימום הנדרש לרוב הרשתות.

טבלה 4.1: *קטגוריות כבלי UTP לפי EIA/TIA 568*

קטגוריה	מהירות העברת נתונים	הערות
1	אין	Voice Only משמש בדרך כלל במערכות טלפון ישנות יותר.
2	4Mbps	LocalTalk
3	10Mbps	Ethernet המינימום הנדרש לרשתות נתונים.
4	16Mbps	Token Ring
5	100Mbps	Fast Ethernet רוב ההתקנות החדשות משתמשות בקטגוריה 5.

אלו הן הקטגוריות המרכזיות שלהן נוספה גם Category 5e. יש עוד קטגוריות. ארגון EIA/TIA הציע קטגוריות נוספות שעדיין לא פורסמו כתקן אלא כהצעה לתקן (proposal) והם: Category 6 ו- Category 7 (שים לב שקטגוריה 7 אינה שייכת למשפחת UTP אלא למשפחת STP).



הערה: כפי שכבר הוזכר, כבלי זוגות שזורים לא-מסוככים (UTP) משמשים להתקנות טלפון. אולם, אין פירוש הדבר בהכרח שאם יש לך שקעים מיותרים במערכת הטלפון שלך תוכל להשתמש בהם לתקשורת נתונים. לתקשורת קול אין דרישות איכות חמורות כל כך כמו לתקשורת נתונים. לפני שאתה משתמש בחיווט קיים, עליך לבדוק שהוא מתאים לשימוש תקשורת נתונים.

כבל זוג שזור לא-מסוכך מספק אמצעי קל ולא יקר לרשתות. החיסרון העיקרי שלו הוא רגישות גבוהה להפרעות ולניחות, ומשמעות הדבר היא שהמרחקים שניתן לכסות עם כבלים מסוג זה מוגבלים מאוד.

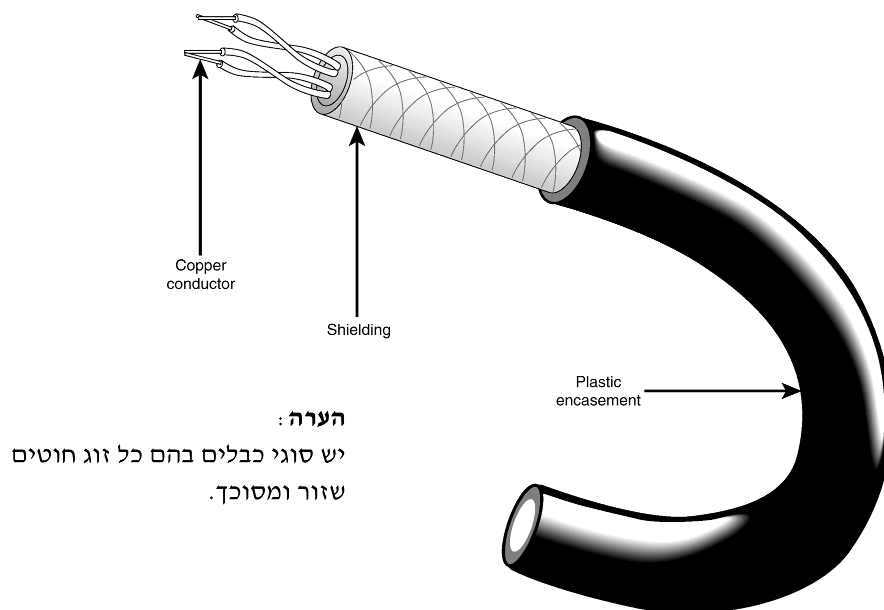
בטבלה 4.2 תמצא את סיכום המאפיינים של כבל UTP.

טבלה 4.2: *סיכום נתונים אודות כבלי UTP*

אורך כבל מירבי	100 מטרים (328 feet).
מהירות העברה	10Mbps בדרך כלל, יכול להיות גם 4-100Mbps.
התקנה/תחזוקה	קל להתקנה ותחזוקה. גמיש מאוד. רכיבים זמינים בקלות.
הפרעות	רגיש מאוד להפרעות (Interference) ודעיכת אותות (Attenuation).
עלות	הזול ביותר מבין סוגי תווך הרשת.

זוג שזור מסוכך
(STP - Shielded Twisted Pair)

ההבדל העיקרי בין כבל **זוג שזור מסוכך - STP** (Shielded Twisted Pair) לבין כבל **זוג שזור לא-מסוכך - UTP**, הוא תוספת סיכוך בתוך הכבל, כפי שמוצג בתרשים 4.6. בדרך כלל, סיכוך זה מורכב מרשת ארוגה (במקרים רבים עשויה נחושת) בין החוטים למעטפת הפלסטיק, אך הוא עשוי לכלול גם מעטפת מתכת סביב הזוגות השונים. בדרך כלל, הרשת הארוגה בעלת הארקה חשמלית, להפחתה נוספת של כמות ההפרעות הנכנסות או היוצאות מהחוט. בגלל צורך זה בהארקה חשמלית, רוב כבלי זוגות שזורים מסוככים (STP) דורשים מחברים מיוחדים.



תרשים 4.6: *כבל זוג שזור מסוכך כולל שכבת סיכוך סביב הזוגות השזורים*

דוגמאות של רשתות המשתמשות ב-STP הן Token Ring של יבמ ו- Apple Talk של אפל. לשני סוגי הרשתות יש מפרטים ברורים לגבי הכבלים בשימוש.

למרות שכבל STP מספק כבל רשת אמין יותר מכבל UTP, הוא סובל מאותן השפעות ניחות כמו UTP, ובדרך כלל לא ניתן להשתמש בו על פני מרחקים העולים על 100 מטרים. STP יקר יותר מ-UTP, והוא עלול להיות קשה יותר להתקנה בגלל קשיחותו והמחברים המיוחדים הדרושים לו.

לפניך סיכום המאפיינים של כבל STP בטבלה 4.3.

טבלה 4.3: *סיכום נתונים אודות כבלי STP*

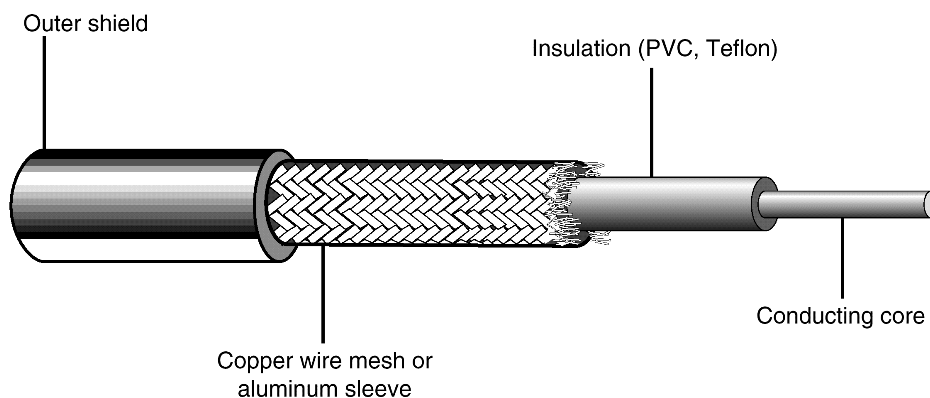
אורך כבל מירבי	100 מטרים (328 feet) (זהה ל-UTP).
מהירות העברה	בדרך כלל 16Mbps, יכול להגיע עד 155Mbps.
התקנה/תחזוקה	בדרך כלל קלה, אולם נדרשים מחברים מיוחדים לכבלים. בנוסף, הכבל בדרך כלל די קשיח.
הפרעות	עמיד בפני הפרעות, אך רגיש לדעיכת אות בדומה ל-UPT.
עלות	יקר יותר מכבל מסוג UTP או מסוג Thinnet coaxial, אולם זול יותר מכבל Thicknet coaxial או כבלי סיב-אופטי.

כבל קואקסיאלי (Coaxial Cable)

רשתות התקשורת הראשונות הופעלו באמצעות כבל קואקסיאלי, המוכר בשם **coax**. כבל קואקסיאלי, שבאופן יחסי אינו יקר וקל להתקנה, היה בשימוש ברוב רשתות המחשבים עד שכבל UTP הפך לזמין. כיום עדיין ניתן למצוא כבלים קואקסיאלים ברשתות רבות.

כפי שניתן לראות בתרשים 4.7, כבל קואקסיאלי מורכב למעשה משני מוליכים המופרדים על ידי שכבת בידוד. הליבה המרכזית היא בדרך כלל חוט נחושת מלא, או מספר סיבי נחושת המלופפים יחד. סביב הליבה נמצא בדרך כלל בידוד פלסטי וסביבו מוליך נוסף בצורת רשת מתכת ארוגה, או מעטפת מתכת. המעטפת חיצונית, עשויה ברוב המקרים מחומר פלסטי, והיא עוטפת את הכבל כולו.

הערה: השם Coax מקורו ב-**Co**mmon **Ax**is, ציר מרכזי.



תרשים 4.7: *כבל קואקסיאלי מורכב משני מוליכים המופרדים זה מזה על ידי שכבת בידוד*

הנתונים מועברים בליבה המרכזית. המוליך החיצוני בעל הארקה חשמלית ומספק סיכוך מפני הפרעות ו- crosstalk. כתוצאה מסיכוך זה, כבל קואקסיאלי הוא בחירה טובה לסביבות שבהן יש הפרעות חשמליות רבות.

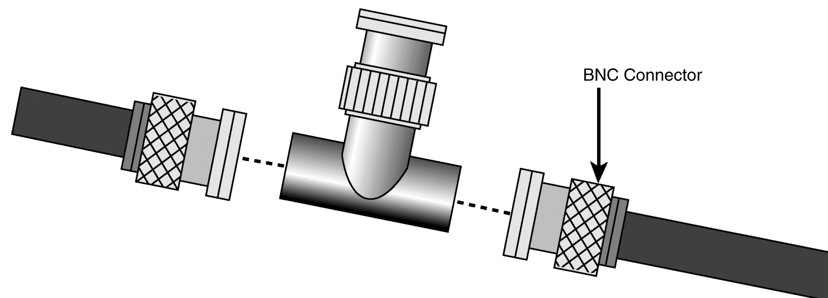
בנוסף, מכיון שחוט הליבה של כבל קואקסיאלי עבה יותר מזה של זוג שזור, הניחות של האות קטן יותר, ולכן ניתן להעביר את הנתונים על פני מרחקים ארוכים יותר. בעוד שכבל זוג שזור מוגבל ל- 100 מטרים, כבל קואקסיאלי יכול להגיע לאורך מירבי של 185 עד 500 מטרים.

קיימים שני סוגים של כבל קואקסיאלי:

- ✯ Thinnet (RG-58)
- ✯ Thicknet (RG-11, RG-8)

כבל Thinnet

מלבד כבל UTP, כבל Thinnet הוא ככל הנראה תווך הרשת הנפוץ ביותר. Thinnet הוא כבל קל משקל וגמיש וניתן להשתמש בו להתקנה מהירה של רשת. בתצורות Ethernet רבות, Thinnet מחובר ישירות ממחשב למחשב, ללא צורך ברכזת (hub), או התקן דומה. כבלי Thinnet משתמשים בדרך כלל ב**מחבר BNC** (British Naval Connector) בכל קצה, כפי שניתן לראות בתרשים 4.8.



תרשים 4.8: *לכבלי Thinnet יש בדרך כלל מחבר BNC בכל קצה*

כבלי Thinnet מסווגים בדרך כלל כחלק ממשפחת כבלי RG-58. סיווג זה, המתואר בטבלה 4.4, פותח על ידי יצרני כבלים ומפרט את עובי הכבל ואת **העכבה** (impedance), או ה**התנגדות** (resistance) לזרם שבכבל.

טבלה 4.4: *כבלים קואקסיאליים נפוצים*

כבל	תיאור	Description
RG-58 /U	50 אוהם, ליבת נחושת מלאה.	Solid Copper Core
RG-58 A/U	50 אוהם, ליבת סיבי נחושת.	Standard Wire Core
RG-58 C/U	מפרט צבאי של RG-58 A/U.	Militery Specification of RG-58A/U
RG-59	75 אוהם, שידורי פס רחב (broadband), כגון טלוויזיה בכבלים.	Broadband transmission
RG-62	93 אוהם, משמש בעיקר ב-ARCnet.	ARCNet Network Cable



הערה: בעת רכישת כבלי רשת, שים לב להבדל בין כבלי RG-58 לבין כבלי RG-59. למרות שהם נראים דומים מאוד, אופן השידור בהם שונה מאוד.



רעיון מפתח

זכור ש- RG-58 משמש עבור Thinnet ברשתות מקומיות (LAN). בנוסף, תלמד בפרק 7 "ארכיטקטורת רשת (שיטות גישור)", שרק RG-58A/U ו- RG-58C/U הם חלק ממפרט IEEE לרשתות Ethernet.

לפניך סיכום המאפיינים של כבל קואקסיאלי Thinnet, בטבלה 4.5.

טבלה 4.5: *סיכום מידע אודות קואקסיאלי Thinnet*

אורך כבל מירבי	185 מטרים (607 רגל).
מהירות העברה	10Mbps.
התקנה/תחזוקה	קל להתקנה, גמיש מאוד.
הפרעות	עמיד בפני הפרעות.
עלות	לא יקר.

כבל Thicknet

כבל Thicknet שימש כתווך עיקרי בימים הראשונים של רשת Ethernet. הליבה המרכזית העבה, שהיא כבל קשיח בקוטר חצי אינץ', מאפשרת לו לשאת אותות למרחקים ארוכים עד 500 מטר (בערך 1,640 רגל). למרות שעדיין ניתן להשיגו, הוא לא נמצא בשימוש נפוץ בגלל קשיחותו ומחירו.

שלא כמו סוגי תווך אחרים שנדונו, כבלי Thicknet (מסוג RG-11 או RG-8) אינם משמשים לחיבור בין מחשבים. במקום זאת, כבל Thicknet עובר במשרד כולו כקו שידרה. בכל מקום שנדרש חיבור, מחובר לכבל **משדר/מקלט** (transceiver) באמצעות **vampire tap** (הנקרא גם **piercing tap**), כפי שניתן לראות בתרשים 4.9. בצורה זו ניתן לחבר כ- 100 צמתים לכבל Thicknet.

מחבר vampire tap יוצר חור בבידוד של הכבל ומאפשר מגע ישיר עם הליבה המרכזית. מחבר drop cable מחבר את המשדר/מקלט לכניסת Attachment unit interface (AUI) בכרטיס ממשק הרשת של המחשב. כניסת AUI היא מחבר בעל 15 פינים הנקרא גם מחבר DB-15.



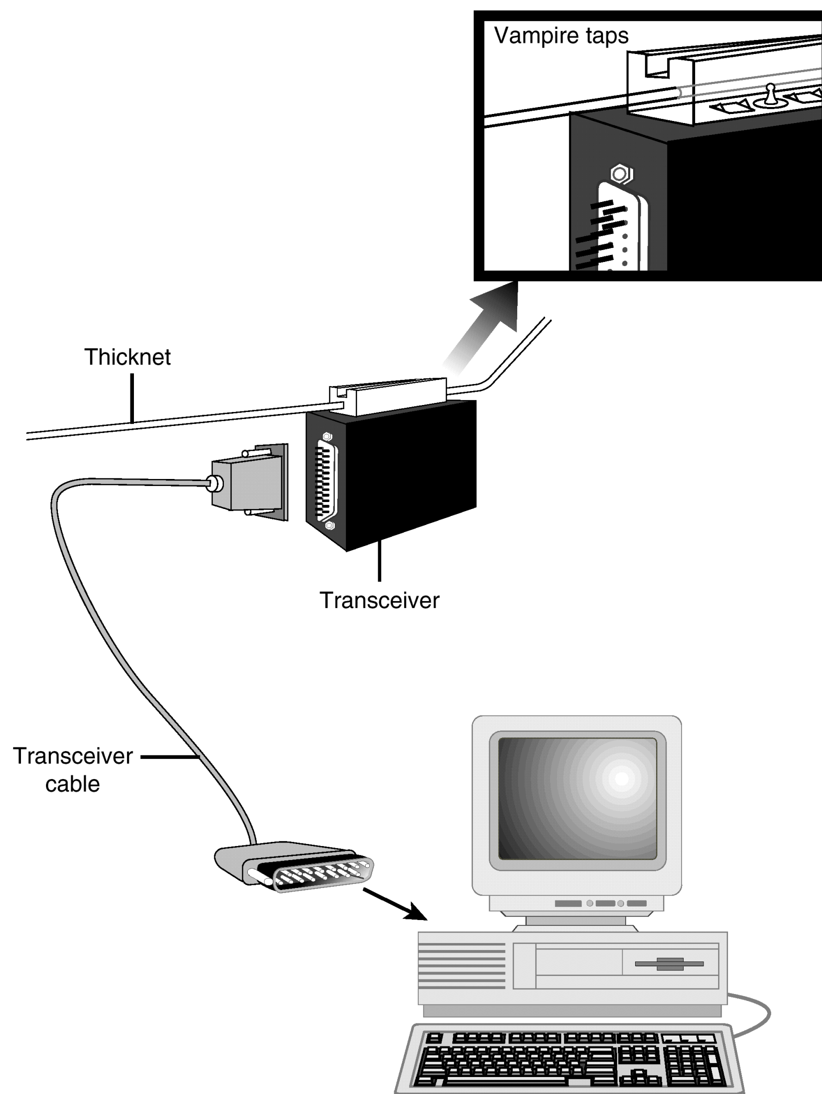
הערה: למרות שכבלי Thicknet כבר אינם בשימוש נרחב כיום, עדיין ניתן למצוא כניסות AUI בכרטיסי ממשק רשת רבים. כניסה זו נקראת לעיתים גם DIX port, על שם החברות שפיתחו אותה: **D**igital, **I**ntel ו- **X**erox.

כפי שכבר הוזכר, כבלי Thicknet כבר אינם נפוצים ברשתות מקומיות, אולם עדיין ניתן למצוא Thicknet כאפיק שידרה המחבר יחד מספר רשתות Thinnet.

בטבלה 4.6 תמצא את סיכום המאפיינים של כבל קואקסיאלי Thicknet.

***טבלה 4.6:** סיכום מידע אודות כבל קואקסיאלי Thicknet*

אורך כבל מירבי	500 מטרים (1,640 רגל).
מהירות העברה	10Mbps.
התקנה/תחזוקה	מבנה קשיח מקשה על התקנה במקומות צרים.
הפרעות	חסין מאוד בפני הפרעות.
עלות	יקר יותר מכל סוגי התווך האחרים, מלבד סיבים אופטיים.

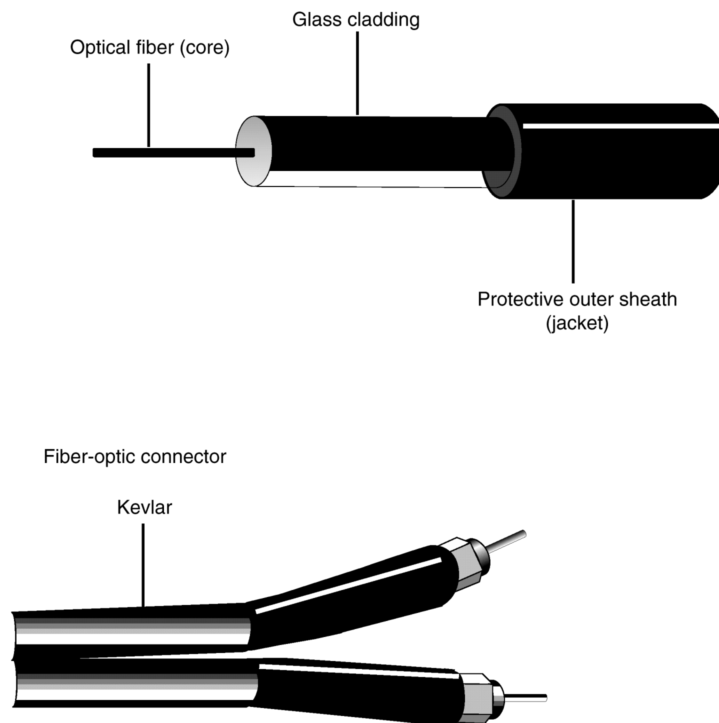


תרשים 4.9: *ברשת המשתמשת בתווך Thicknet, מחשבים מתחברים לאפיק שדרה Thicknet באמצעות vampire tap ו- drop cable (כבל סעף)*

כבל סיב-אופטי (Fiber-Optic)

שלא כמו בסוגי הכבלים האחרים שנדונו, הנתונים בכבל סיב-אופטי מועברים בצורת **אור**, ולא בצורת אות חשמלי. זו הסיבה שכבלי סיב-אופטי **אינם רגישים** כלל להפרעות האלקטרומגנטיות המפריעות לאות בחוטי נחושת. בנוסף, מכיון שכבלי סיב-אופטי אינם מחוללים הפרעות אלקטרומגנטיות, כמעט בלתי אפשרי לאדם מבחוץ "לצותת" לאות שעובר בכבל. כבלי סיב-אופטי בטוחים מאוד ומהירים מאוד, אך גם יקרים מאוד.

כבלי סיב-אופטי מיוצרים עם סיב מרכזי מזכוכית (או מחומר אחר), המוקף בשכבת זכוכית הנקראת **cladding**, וממעטפת חיצונית מפלסטיק להגנה, כפי שניתן לראות בתרשים 4.10.



***תרשים 4.10:** בכבל סיב-אופטי ליבת זכוכית מרכזית עטופה בשכבת זכוכית נוספת הנקראת cladding*

מכיון שכל סיב יכול להעביר אור רק בכיוון אחד, דרושים בכבלי סיב-אופטי שני סיבים, שלכל אחד מהם cladding ומעטפת מגן משלו. סיב אחד שולח נתונים מהמחשב לרשת. השני מעביר נתונים מהרשת למחשב.

התקנת רשתות סיבים אופטיים עלולה להיות מסובכת בשל הצורך להניח את הכבלים בכוונון מדויק (align) ובגלל קשיחות הכבלים.



הערה: את כבלי סיב-אופטי ניתן לחלק לסוגים שונים: כבלי single mode שהם יקרים יותר ומיועדים בעיקר לשימוש עם לייזרים. כבלי multi mode שיכולים לפעול עם דיודות פולטות אור - LED (Light Emitting Diode).

בטבלה 4.7 תמצא את סיכום המאפיינים של כבל סיב-אופטי.

טבלה 4.7: *סיכום מידע אודות כבל סיב-אופטי*

אורך כבל מירבי	2 קילומטר (6,562 רגל).
מהירות העברה	בדרך כלל 100Mbps, למרות שהודגמו מהירויות עד 2Gbps.
התקנה/תחזוקה	קשה.
הפרעות	לא נתון כלל להפרעות אלקטרומגנטיות.
עלות	היקר ביותר מבין תווכי הרשת.

בחירת הכבל המתאים

עם אפשרויות רבות כל כך, בחירת הכבל המתאים עלולה להיות משימה קשה. יש לשקול מספר גורמים וביניהם:

- מהן מגבלות העלות הקיימות?
- כמה מחשבים יחוברו יחד?
- מה האורך הנדרש לכבלים?
- מה רמת התעבורה הצפויה ברשת?
- עד כמה חשובה האבטחה של הרשת?
- אילו בעיות התקנה (מעברים צרים וכד׳) יעמדו בפניך?
- מה מהירות הרשת הרצויה?

בעולם שבו העלות אינה חשובה וקל לחווט את כל המחשבים והמשרדים, מספקים כבלי סיב-אופטי ללא ספק את הרמה הגבוהה ביותר של מהירות ואבטחה. אולם מקרים כאלה נדירים מאוד.

אם אתה מחפש רשת זולה, קלה ומהירה, פתרון המבוסס על UTP ורכזת (hub), או על Thinnet לבד יאפשרו לך חיבור מהיר.

כיום, תצורה נפוצה בסביבת המשרד מבוססת על כבלי UTP ברשת תקשורת מקומית (LAN) משרדית. אפשר גם למצוא כבלי סיב-אופטי הפועלים כאפיקי שידרה לחיבור רשתות מקומיות משרדיות אלו יחד, כדי ליצור רשת מרחבית (WAN).

בטבלה 4.8 תמצא את סיכום המאפיינים של תווכי רשת פיסיים המתוארים בפרק זה.

טבלה 4.8: *השוואה בין תווכי הרשת השונים*

אמצעי	**אורך כבל מירבי**	**מהירות העברה**	**התקנה**	**רמת הפרעות**	**עלות**
UTP	100 מטרים (328 רגל)	10-100Mbps	קלה	גבוהה	נמוכה ביותר
STP	100 מטרים (328 רגל)	16-155Mbps	די קלה	נמוכה	ביניים
Thinnet	185 מטרים (607 רגל)	10Mbps	קלה	נמוכה	נמוכה
Thicknet	500 מטרים (1,640 רגל)	10Mbps	קשה	נמוכה יותר	גבוהה
Fiber-Optic	2000 מטר (6,562 רגל)	100Mbps - 2Gbps	קשה	אין	גבוהה

סיכום

בשכבה הפיסית של מודל OSI, תווך הרשת עסוק בהעברה של נתונים בין מחשבים. נתונים אלה מקודדים לאות דיגיטלי (שידור **פס-בסיס** - baseband) או לאות אנלוגי (שידור **רחב פס** - broadband) ונשלחים על פני תווך הרשת.

מרבית הכבלים נתונים לסוג כלשהו של **ניחות** או **דעיכת אות** (attenuation), ואיכות האות נחלשת ככל שהאות מתקדם בכבל. דעיכת אות זו מושפעת מה**עכבה** (impedance), או ה**התנגדות** (resistance), של הכבל. כבלים יוצרים **הפרעות** (interference), העלולות להפריע לכבלים או התקנים קרובים אחרים. סוג מסוים של הפרעה הנקרא crosstalk מתרחש כאשר שני כבלים מונחים קרוב מאוד זה לזה. להפחתת ההפרעות, סוגים מסוימים של כבלים משתמשים בשכבת **סיכוך** (shielding).

תווכי רשת מסווגים באופן גס לשלושה סוגים: זוג שזור, קואקסיאלי וסיב-אופטי.

כבלי זוג שזור מורכבים ממספר זוגות חוטי נחושת המאוגדים יחד. בכל זוג, החוטים הבודדים מלופפים יחד באופן המקטין את ה-crosstalk. כבלי זוג שזור זמינים בשתי גרסאות: לא-מסוכך (UTP) ומסוכך (STP).

כבל זוג שזור לא-מסוכך, המוכר כ-UTP, הוא אמצעי הרשת הנפוץ ביותר והקל ביותר לשימוש. UTP משמש גם למערכות טלפון, גמיש מאוד ורכיביו זמינים בקלות. UTP מסווג לחמש קטגוריות, כאשר קטגוריה 3 היא המינימום הנדרש לרישות מחשבים וקטגוריה 5 מאפשרת את מהירות ההעברה הגבוהה ביותר. UTP רגיש מאוד להפרעות ולדעיכת אות. אורך הכבל המירבי הוא 100 מטר.

כבל זוג שזור מסוכך, או STP, כולל שכבת סיכוך רשת ארוגה המפחיתה את ההפרעות ומאפשרת מהירות העברה גבוהה מעט מ-UTP. STP גמיש פחות והתקנתו קשה יותר מ-UTP, ואף הוא מוגבל לאורך של 100 מטר. Token Ring של יבמ ו- AppleTalk של אפל הן דוגמאות לרשתות המשתמשות ב-STP.

כבל קואקסיאלי, או "coax", מורכב מליבה פנימית המשדרת את הנתונים ושכבה חיצונית של סיכוך מוליך חשמלית להפחתת הפרעות. לכבל קואקסיאלי ליבה עבה יותר מאשר לזוג שזור, הוא רגיש פחות לדעיכת האות ויכול להעביר נתונים על פני מרחקים ארוכים יותר. כבל קואקסיאלי מתחלק לשני סוגים : Thinnet ו- Thicknet.

כבל Thinnet, כמו UTP, קל להתקנה וזול יחסית. הוא משדר נתונים ב- 10Mbps ובעל אורך מירבי של 185 מטר. חיבור לכבלי Thinnet נעשה בעיקר באמצעות מחברי BNC.

כבל Thicknet היה הכבל המקורי ששימש ברשתות Ethernet, הוא בעל ליבה עבה יותר המאפשרת לשדר נתונים עד 500 מטר. בעת חיבור לכבל Thicknet, משתמשים ב- vampire tap לניקוב הכבל וחיבור ישיר לליבה הפנימית, וכן כבל מקלט/משדר (מקמ"ש) ושקע AUI לחיבור המקמ"ש עם מתאם הרשת במחשב.

כבלי סיב-אופטי (Fiber-optic) משתמשים באור במקום באותות חשמליים להעברת נתונים. כבלי סיב-אופטי יכולים להעביר נתונים למרחק של עד שני קילומטר ובמהירויות גבוהות מאוד. תמורת יכולת זו משלמים במחיר של הכבלים מסוג זה - הם יקרים יותר בעלות הכבל אך צריך לעשות חישוב מדוייק לבדיקת העלות לאורך חיי המוצר.

לסיום, חשוב שסוגי הכבלים המותקנים בתקרה או בקירות, יהיו מוגנים בעת דליקה (**plenum**-grade). יש לבדוק את נוהלי בטיחות האש המקומיים לפני התקנת כבלים.

5

חיבורי אלחוט

עם הגידול ברשתות ובניידות המשתמשים ברשתות, חיבורים באמצעות כבלים מסורתיים אינם תמיד אפשרות מעשית. אמצעים אלחוטיים מספקים מנגנון לביצוע חיבורים אלה ללא כבלים. עד סוף פרק זה תהיה מסוגל:

- ✯ לזהות את הסוגים השונים של טכנולוגיות אלחוט,
- ✯ להבין תקשורת רדיו כפי שהיא מתייחסת לרשתות,
- ✯ לתאר תקשורת מיקרוגל,
- ✯ להסביר את השיטות לחיבור מחשבים באמצעות טכנולוגיית אינפרא-אדום.

סוגי חיבור אלחוטי

סוגי תווך אלחוטיים יכולים לספק את היכולת לאספקת חיבורי רשת מרוחקים וגם חיבור רשתות על פני מרחקים ארוכים.

תווכים אלחוטיים מתחלקים באופן גס לשלושה סוגים:

- ✯ רדיו,
- ✯ מיקרוגל,
- ✯ אינפרא-אדום.

כל סוג יוסבר בפירוט בסעיפים הבאים, אולם תחילה עליך להכיר את הספקטרום האלקטרומגנטי.

הספקטרום האלקטרומגנטי

כל תמסורת של אנרגיה מתרחש בצורת גלים **בספקטרום האלקטרומגנטי** (electromagnetic spectrum). **תדר אלקטרומגנטי** (electromagnetic frequency) הוא מספר מחזורי הגל בשנייה ונמדד במונחים של **הרץ** (**Hz** - hertz).

אתה מכיר בוודאי סוג זה של מידה ממחוג הרדיו ברכב שלך. תחנות רדיו AM פועלות בתחום התדרים 530-1600 Kilohertz (1KHz = 1,000Hz), ואילו תחנות רדיו FM משתמשות בתחום 88-108 Megahertz (1MHz = 1,000,000Hz). בנוסף, אם תסתכל כמעט על כל מכשיר חשמלי ביתי, תמצא בדרך כלל שהוא מיועד לעבוד ב- 50HZ בישראל ובאירופה, וב- 60Hz בארה״ב. לסיום, תחום תדרי השמיעה של בני האדם נע בתחום שבין 30Hz לבין 20KHz.

תדר התמסורת משפיע הן על כמות הנתונים שניתן לשדר והן על המהירות שבה מתבצעת התמסורת. תדרים נמוכים יכולים לעבור מרחקים ארוכים רצופי מכשולים, אולם כמות הנתונים שניתן לשלוח מוגבלת מאוד. ככל שהתדר של האות גובר, כמות הנתונים שהוא יכול להעביר גדלה בהתאם. ככל שהתדר ממשיך לגדול תוכל לשלוח כמות גדולה של נתונים, אך עדיין תוך הגבלה לתקשורת **בקו-ראייה** (line of sight), שבו המשדר והמקלט נמצאים בטווח ראייה זה מול זה.



רעיון מפתח

זכור זאת כך: תדר נמוך = קצב העברת נתונים נמוך על פני מרחקים ארוכים.

תדר גבוה = קצב העברת נתונים גבוה על פני מרחקים קצרים.



הערה: רוב המחשבים המשדרים ברשת מקומית על פני כבלים פועלים בקצה הנמוך של הספקטרום, ומשתמשים באותות חשמליים פשוטים או באותות בתדר רדיו (RF - Radio Frequency). כבלי סיב-אופטי פועלים בקצה השני של הספקטרום, ומשתמשים בתדרים הגבוהים של אינפרא-אדום או אור נראה.

רדיו

תדר הרדיו (radio frequency - RF) שבתחום הספקטרום האלקטרומגנטי משתרעת על פני תחום התדרים מ- 10KHz עד 1GHz (gigahertz).

השימוש בתדרי הרדיו בכל מדינה מבוקר על ידי רשויות השלטון. בארץ עושה זאת משרד התקשורת ובארה״ב אחריות זו מוקצית ל- FCC (Federal Communications Commission).

אם השתמשת פעם בטלפון אלחוטי או צעצוע עם שלט רחוק, קרוב לוודאי שהוא פעל בתחום 902-928MHz. תחום תדרים אלה זמין כבר זמן רב ומשמש כיום להתקנים רבים, ולכן גובר השימוש בתחום 2.4GHz. מכיון שעלות הציוד עולה גם היא עם התדרים הגבוהים, תחום 5.72GHz נמצא בשימוש מועט בלבד כיום.

שימוש בתדרי רדיו ברשת מחשבים להעברת נתונים מחייבת שלכל הֶתקֵן יהיו הן **אנטנה** (antenna) והן **משדר/מקלט** (transceiver). בהתאם למרחק ולתדרים שבשימוש, האנטנה עשויה להיראות כמו זו של רדיו רגיל, טלפון סלולרי, או מכשיר טלוויזיה. המשדר/מקלט הוא הֶתקֵן שיכול לשדר ולקלוט נתונים.

תקשורת רדיו המשמשת רשתות מחשבים מקומיות מתחלקת לשלוש קטגוריות:

- הספק נמוך, תדר יחיד - Low Power, Single Frequency
- הספק גבוה, תדר יחיד - High Power, Single Frequency
- ספקטרום פרוש - Spread Spectrum

סוגים שונים אלה יידונו בסעיפים הבאים.

הספק נמוך, תדר יחיד (Low Power, Single Frequency)

בתרחיש זה, הן ה**משדר** (Transmitter) והן ה**מקלט** (Receiver) למעשה "**מכוּוָנים**" (tuned) לתדר אחד שבו מתרחשת כל תקשורת הנתונים. ההספק הנמוך של מערכות אלו פירושו בדרך כלל שהאות מונחת במהירות, וניתן להשתמש בו באזור מוגבל בלבד. בהתאם לתדרים שבשימוש, קירות ומכשולים אחרים יכולים לחסום אותות אלה ולמנוע תקשורת. הפרעות מהתקנים אחרים עלולות להתרחש בקלות, במיוחד בתחום 902MHz העמוס. רשתות LAN המבוססות על טכנולוגיות אלו רגישות מאוד גם להאזנה, למרות שההספק הנמוך מגביל את התחום שבו מישהו יכול לקלוט את האות.

טבלה 5.1: *סיכום המידע אודות רשתות רדיו בהספק נמוך ותדר יחיד*

תדרים:	הכל אפשרי אך בדרך כלל נמוך בתחום ה-GHz
טווח מירבי:	עשרות מטרים
מהירות שידור:	יכולה להיות 1-10Mbps
התקנה/תחזוקה:	קלה יחסית להתקנה
הפרעות:	רגישה מאוד להפרעות
עלות:	בינונית
אבטחה:	רגישות גבוהה לציתות, למרות שהאות מוגבל לתחומי הבניין בשל ההספק הנמוך

הספק גבוה, תדר יחיד (High Power, Single Frequency)

כפי שהשם מרמז, רשתות אלו פועלות בהספק גבוה יותר ולכן הן מאפשרות שידור על פני אזור רחב. בדרך כלל רשתות מסוג זה משדרות עד האופק, או מעבר לאופק, על ידי שימוש ב**מגברים** (repeaters) ו/או **החזרה** (bouncing) של האות מהאטמוספירה. למרות שהדבר עשוי להתאים לתקשורת עם משתמשים ניידים, יש לכך מחיר. רשתות בהספק גבוה ובתדר יחיד דורשות בדרך כלל ציוד שידור יקר יותר, במיוחד עם אנטנות ומגברים, ודורשות גם רישוי לתקשורת. מפעילי הציוד חייבים להיות מורשי FCC (בארה"ב) ולתחזק את כל הציוד בהתאם לנהלים.

גם האבטחה היא נושא לדאגה ברשת מסוג זה. כאשר האות משודר על פני אזור רחב, תיתכן אפשרות שהוא ייקלט על ידי זרים המעוניינים לצותת לרשת שלך.

לפניך טבלה 5.2 בה סיכום המאפיינים של רשתות רדיו בעלות הספק גבוה ותדירות יחידה.

טבלה 5.2: *סיכום המידע אודות רשתות רדיו בהספק גבוה ותדר יחיד*

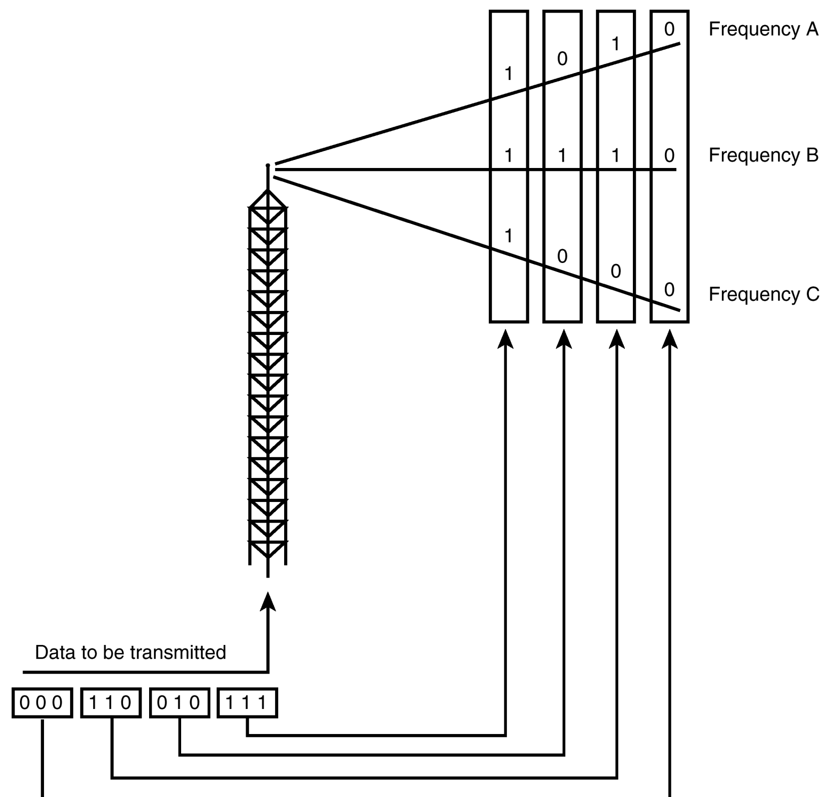
תדרים:	הכל אפשרי אולם בדרך כלל נמוך בתחום ה-GHz
טווח מירבי:	תלוי בהספק ובתדירות המשדרים. יכול להיות קו-ראיה או מעבר לאופק
מהירות שידור:	יכולה להיות 1-10Mbps
התקנה/תחזוקה:	קשה. דרוש רישוי
הפרעות:	רגישות גבוהה להפרעות
עלות:	בינונית עד יקרה מאוד
אבטחה:	רגישות גבוהה לציתות, בעיקר בגלל שהאות משודר לאזור רחב

ספקטרום פרוש (Spread Spectrum)

תקשורת מסוג **ספקטרום פרוש** (spread spectrum) פותחה כדי לענות על החסרונות הרבים של תקשורת בתדר יחיד (הן בהספק נמוך והן בהספק גבוה). במקום להשתמש בתדר יחיד, רשתות מסוג ספקטרום פרוש משתמשות במספר תדרים בו-זמנית. הדבר משפר אמינות ומגביר את ההתנגדות להפרעות. בנוסף לכך שהשימוש במספר תדרים מקשה על ציתות, ניתן להדק את האבטחה עוד יותר על ידי הצפנת תקשורת הנתונים.

קיימים שני סוגים עיקריים של שידורי ספקטרום פרוש (spread spectrum):

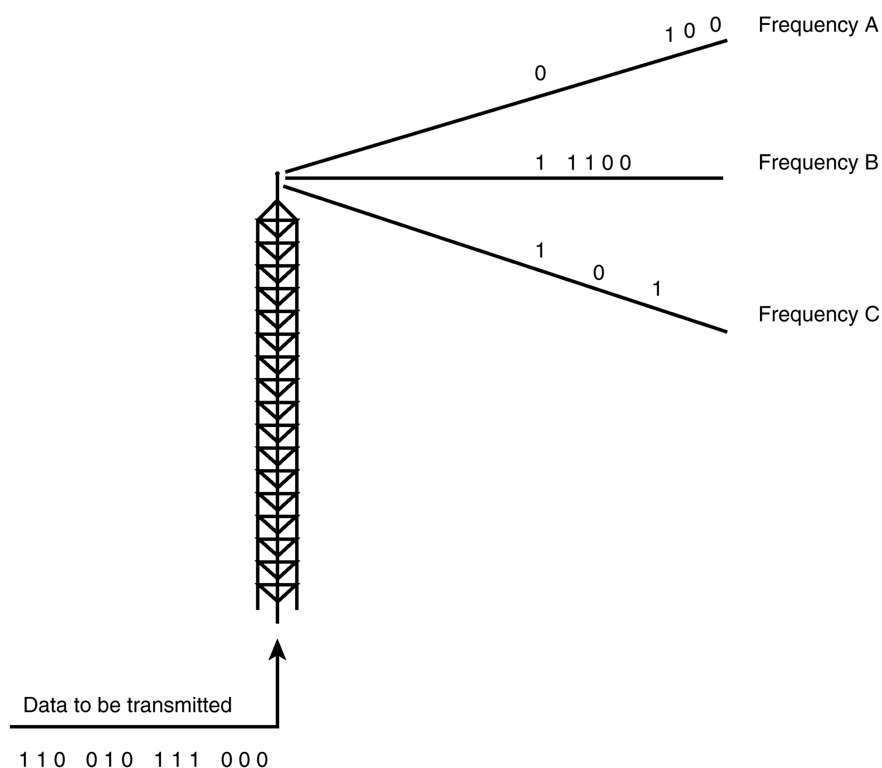
- direct-sequence modulation (אפנון רציף),
- Frequency-hopping (דילוג בתדר).



__תרשים 5.1:__ אפנון רציף (direct sequence modulation) כרוך בשידור בו-זמני של נתונים במספר תדרים

אפנון רציף (direct-sequence modulation) מחלק את הנתונים לחלקים הנקראים **שבבים** (chips) ומשדר אותם במספר תדרים שונים (ראה תרשים 5.1). התחנה הקולטת יודעת לאילו תדרים להקשיב ומרכיבה מחדש את השבבים המתקבלים למנות (packets) נתונים. ניתן להדק את האבטחה על ידי שידור נתוני דמה יחד עם הנתונים האמיתיים, ועל ידי שידור נתוני דמה בתדרי דמה אחרים. התחנה המקבלת יודעת אילו תדרים תקפים וכיצד לקבוע איזה שבבים תקפים. גורם המעוניין לצותת יצטרך למצוא את כל התדרים, ויצטרך להבחין בין הנתונים האמיתיים למדומים.

רשתות מסוג זה פועלות בדרך כלל בתדרים שאינם בפיקוח (unregulated use), והן יכולות להגיע למהירויות שידור של 2-6Mbps.



***תרשים 5.2:** בדילוג בתדר (Frequency-hopping) נתונים משודרים בתדרים שונים לפי לוח זמנים קבוע מראש*

דילוג בתדר (Frequency-hopping) שמוצג בתרשים 5.2, ממתג נתונים בין מספר תדרים. המשדר והמקלט מסונכרנים לשימוש באותם תדרים **בפרקי זמן** (time slots) שנקבעו מראש. התזמון קריטי, ושני הצדדים חייבים להיות מסונכרנים בדיוק כדי שתהיה תקשורת. מסיבה זו קשה לגורם חיצוני לצותת לרשת מסוג זה. כדי לעשות זאת, הוא יצטרך לדעת את הערכים שנקבעו מראש.

רשתות המדלגות בתדר מספקות יותר אבטחה מאשר רשתות הפועלות באפנון רציף, אולם במחיר הפחתת המהירות. למרות שהן יכולות להגיע למהירויות של עד 2Mbps, רשתות המדלגות בתדר מוגבלות בדרך כלל למהירויות נמוכות יותר.



רעיון מפתח

מערכות רדיו של ספקטרום פרוש (spread spectrum) משדרות נתונים במספר תדרים ובטוחות יותר מאשר מערכות רדיו בתדר יחיד.

לפניך טבלה 5.3 בה סיכום המאפיינים של רשתות רדיו בשיטת ספקטרום פרוש.

טבלה 5.3: סיכום המידע אודות רשתות רדיו בשיטת spread spectrum

תדרים:	בדרך כלל 902-928MHz. חלק ב- 2.4GHz
טווח מירבי:	תלוי בהספק ובתדרים. במקרים רבים מוגבל, אבל יכול להיות יותר ממספר מיילים
מהירות שידור:	מערכות 902MHz direct sequence מציעות 2-6Mbps. מערכות GHz מאפשרות מהירויות גבוהות יותר. דילוג תדרים בדרך כלל איטי יותר (מתחת ל- 1Mbps)
התקנה/תחזוקה:	תלוי בתכנון. יכול להיות פשוט עד מורכב
הפרעות:	עמיד בפני הפרעות
עלות:	זול יחסית
אבטחה:	עמיד מאוד בפני ציתות

מיקרוגל (Microwave)

מערכות תקשורת **מיקרוגל** (microwave), המשתמשות בתדרים הגבוהים יותר של תחום הג׳יגה הֶרץ הנמוך, מאפשרות קצב שידור נתונים גבוה יותר. אולם כדי לעשות זאת, המשדר והמקלט חייבים להיות בטווח ראייה זה מול זה. תקשורת מיקרוגל דורשת בדרך כלל שימוש בתדרים מורשים ולכן יקרה יותר ממערכות רדיו.

קיימים שני סוגים של תקשורת מיקרוגל: **קרקעי** (terrestrial) **ולוויני** (satellite).

מיקרוגל קרקעי (Terrestrial Microwave)

אם בעת נסיעה בכביש מהיר הבחנת במגדלים עם ״צלחות״ לווין בראשיהן (כמו למשל ליד זיכרון יעקב, או בגבעתיים), ראית מערכות תקשורת מיקרוגל קרקעי. מערכות אלו משתמשות באות ממוקד מאוד בתדר גבוה לקישור בין שני אתרים. כל אתר חייב להשתמש ב**אנטנה פרבולית כיוונית** (directional parabolic antenna) וחייב להיות בקו-ראייה של האנטנה השנייה, כפי שמוצג בתרשים 5.3. **מגדלי ממסר** (relay towers) יכולים לשמש להעברת האות על פני מרחקים ארוכים יותר.

מערכות מיקרוגל קרקעיות משמשות בדרך כלל לקישור רשתות על פני מרחקים גדולים שבהם כבלים אינם מעשיים, או שעלותם אינה מעשית. בגלל הדרישה לקו-ראייה, מציאת מקומות מתאימים למגדלי ממסר עלולה להיות בעייתית.

התקנה של מערכות מיקרוגל קרקעיות קשה יחסית, בעיקר בגלל העובדה שהאנטנות חייבות להיות מיושרות (aligned) בקפידה כדי לקלוט את האות. בנוסף, השימוש בתדרים מורשים מציב דרישות על הציוד שבשימוש ועל הצוות שמפעיל את הציוד.



תרשים 5.3: *תקשורת מיקרוגל קרקעית יכולה להתקיים בין שני בניינים*

מערכות מיקרוגל בהספק נמוך יכולות גם לשמש בסביבות רשתות מקומיות קטנות. לכל מחשב יהיה משדר קטן שיתקשר עם רכזת מיקרוגל שנמצאת במקום מרכזי גבוה כלשהו, למשל התקרה. בכל מקרה, צריך להיות קו-ראייה בין כל משדר לרכזת.



רעיון מפתח

בעוד שמערכות מיקרוגל קרקעיות מאפשרות תקשורת על פני מרחקים גדולים, תחנות השידור והקליטה חייבות להיות בקו-ראייה ברור ביניהן.

תמצא בטבלה 5.4 את הסיכום של המאפיינים של תקשורת מיקרוגל קרקעית.

טבלה 5.4: *סיכום המידע אודות תקשורת מיקרוגל קרקעית*

תדרים:	בדרך כלל 4-6GHz או 21-23GHz
טווח מירבי:	תלוי בהספק ובתדרים. במקרים רבים מוגבל, אבל יכול להיות יותר ממספר קילומטרים
מהירות שידור:	תלוי בתדרים, אך במקרים רבים 1-10Mbps
התקנה/תחזוקה:	די קשה
הפרעות:	משתנה עם ההספק, גודל האנטנה, והתדרים שבשימוש. בטווחים קצרים ההפרעות אינן מהוות בדרך כלל בעיה. תנאי אקלים (גשם, ערפל) עלולים להשפיע על מערכות במרחקים גדולים יותר או בתדרים גבוהים יותר
עלות:	בינונית עד גבוהה
אבטחה:	רגישות לציתות. האות בדרך כלל מוצפן

מיקרוגל לוויני (Satellite Microwave)

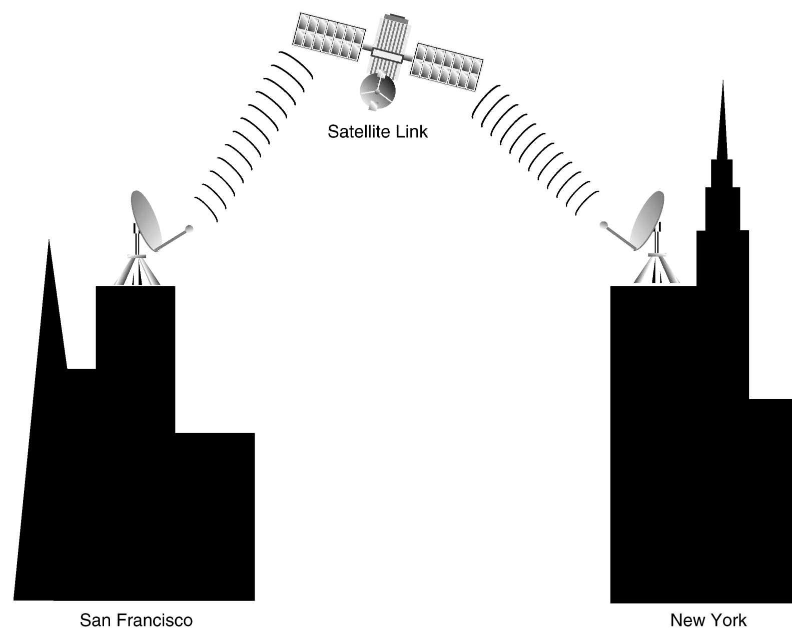
כמו מערכות מיקרוגל קרקעיות, מערכות תקשורת לוויינית משתמשות באנטנות פרבוליות כיווניות וכל אנטנה חייבת להיות בקו-ראייה של חברתה. ההבדל העיקרי הוא, שאנטנה אחת נמצאת על הקרקע והאחרת נמצאת בחלל, על לווין גיאוסינכרוני בגובה 50,000 ק״מ (22,300 מייל) מעל כדור הארץ. לווינים אלה נמצאים במסלול, בגובה ובמהירות שבהם הם נשארים קבועים ביחס לכדור הארץ. זוהי השיטה המשמשת לשידור תמונות טלוויזיה מרחבי העולם.

עבור תקשורת רשתות, האות מרשת תקשורת מקומית ישודר ללווין ומשם יוחזר לאזור מסוים של כדור הארץ (ראה תרשים 5.4). בקצה המקבל, אנטנה נוספת תמיר את האות מהלווין ותשדר את הנתונים הלאה לרשת המקומית שבאתר המקבל. אם שני האזורים קרובים זה לזה, השידור יכול לעבור בלווין אחד. אם אתה משדר לאתר רחוק מאוד, האות יכול להתקבל על ידי לווין אחד ואז לעבור ללווין אחר לשידור חזרה לקרקע.

בגלל המרחק הגדול מהקרקע ללווין ובחזרה, **השהיות מעבר** (propagation delays) שבין 0.5 לבין 5 שניות הן תופעה נפוצה. התופעה מתרחשת הן בשידור לאתר קרוב, והן בשידור לאתר שבצדו השני של כדור הארץ.

התקנת מערכת תקשורת לווינית לקישור בין שתי רשתות היא תהליך מורכב ומסובך מאוד. כמובן ששידור לווין הוא מעבר להישג ידם של רוב הארגונים, מלבד אולי העשירים ביותר שבהם, וגם חכירת תדירויות על לווינים קיימים יקרה מאוד. לאחר השגת תדרים, קביעת התצורות של הלווין ושל תחנות הקרקע היא נושא טכני מורכב מאוד ועדיף להשאירו לאנשים שהוכשרו בתחום.

מכיון שהאות המשודר מהלווין יכול לכסות אזור גיאוגרפי גדול, הציתות קל יחסית. לכן רוב שידורי הלווין מוצפנים בדרך זו, או אחרת.



תרשים 5.4: *תקשורת מיקרוגל לוויינית מאפשרת תקשורת על פני מרחקים ארוכים*

בטבלה 5.5 תמצא את סיכום מאפייני תקשורת מיקרוגל לוויינית.

טבלה 5.5: *תקשורת מיקרוגל לוויינית*

תדרים:	בדרך כלל 11-14GHz
טווח מירבי:	כלל עולמי
מהירות שידור:	תלוי בתדרים, אך בדרך כלל 1-10Mbps
התקנה/תחזוקה:	קשה, עד קשה מאוד
הפרעות:	רגישה להפרעות אלקטרומגנטיות, **חסימה** (jamming), ותנאי אקלים
עלות:	יקרה מאוד
אבטחה:	רגישה מאוד לציתות, בדרך כלל האות מוצפן

אינפרא-אדום (Infrared)

במעלה הספקטרום האלקטרומגנטי, תדרי **אינפרא-אדום** (infrared - IR) ממלאים את התחום שבין 100GHZ לבין 1,000THz (terahertz), מעט מתחת לתחום האור הנראה. הטכנולוגיה המשמשת לרישות אלחוטי דומה מאוד לטכנולוגיות אינפרא-אדום המשמשות למערכות שלט רחוק עבור טלוויזיות או מערכות סטריאו. **דיודה פולטת אור - LED** (Light Emitting Diode) או לייזר משמשים כמקור אור לשיגור אלומת אור בין המשדר למקלט.

טכנולוגיות אינפרא-אדום פועלות בתדרים גבוהים המאפשרים מהירויות העברת נתונים גבוהות. אולם מכיון שהן קרובות לתדרים של אור נראה, הן סובלות מבעיות שידור רבות המאפיינות מקורות אור רגילים. בדיוק כפי שלא ניתן לראות טלוויזיה דרך קיר, גם אותות אינפרא-אדום אינם יכולים לעבור דרך קירות או עצמים גדולים אחרים. כשיש אור חזק ליד הטלוויזיה, הוא עלול להפריע ליכולת שלך לראות את התמונה. באופן דומה, אות אינפרא-אדום עלול להיחלש על ידי נוכחות מקור אור נוסף.



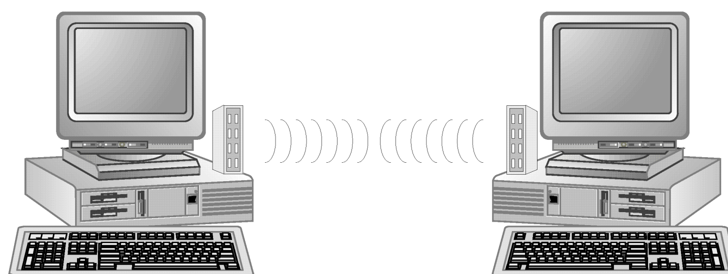
הערה: תוכל לשאול כיצד הפרעה זו מתרחשת ללא מקור אור אינפרא-אדום נוסף באזור. אולם, אפילו נורות להט רגילות עלולות להפריע לתקשורת באינפרא-אדום, וזאת בגלל שנורות להט רגילות פולטות גם אינפרא-אדום בנוסף לאור הנראה.

יתרון אחד של רשתות אינפרא-אדום הוא שהן אינן רגישות להפרעות האלקטרומגנטיות מהסוג שמפריע לתווכי רשת אחרים, כגון כבלים קואקסיאלים. כמו כבל סיב-אופטי, מערכות אינפרא-אדום יכולות לשמש בסביבות עם הפרעות, כמו למשל מנועים חשמליים או קווי מתח.

קיימות שתי טכנולוגיות תקשורת אינפרא-אדום: **נקודה-לנקודה** (point-to-point) **ושידור** (broadcast).

אינפרא-אדום נקודה-לנקודה (Point-to-Point Infrared)

מערכות אינפרא-אדום נקודה-לנקודה משתמשות באלומה צרה וממוקדת מאוד של אנרגיה לקישור שני אתרים במהירויות שידור גבוהות. בסביבת רשת מקומית נמצא מחשבים ניידים רבים **ויומנים אלקטרוניים אישיים - PDA** (personal digital assistants) שמשתמשים בכניסות אינפרא-אדום ל"עגינה" עם מערכות מחשב שולחניות, או עם התקנים היקפיים אחרים. למרות שהתהליך דורש יישור מדויק של כניסות אינפרא-אדום על המחשב הנייד ועל יחידת העגינה, התהליך יכול למנוע את הצורך בחיבור כבלים כדי להתחבר לרשת. ניתן גם להוסיף מתאמי אינפרא-אדום למחשבים אישיים רגילים, כפי שניתן לראות בתרשים 5.5.



תרשים 5.5: *תקשורת אינפרא-אדום נקודה-לנקודה מאפשרת תקשורת בין שני מחשבים הנמצאים בקרבה פיסית זה לזה*

טכנולוגיות לייזר הפועלות בתחום אינפרא-אדום נוצרו כחלופה אפשרית למערכות מיקרוגל קרקעיות. כאשר קיים קו-ראייה, מערכות מבוססות לייזר יכולות לקשר בניינים במרחק אלפי מטרים. **שלא** כמו מערכות מיקרוגל קרקעיות, פתרונות מבוססי לייזר **אינם** מחייבים רישוי (של FCC למשל), ולכן קל יותר להתקין ולתחזק אותן בהשוואה למערכות מיקרוגל דומות.

באשר לאבטחה, שידורי אינפרא-אדום נקודה-לנקודה קשים יחסית לקליטה. אלומת האנרגיה כל כך ממוקדת עד שכמעט יש צורך להפריע לזרימת הנתונים כדי לצותת לתקשורת. הפרעה זו תורגש על ידי הקצה המקבל.

טבלה 5.6 מספקת את סיכום המאפיינים של מערכות אינפרא-אדום נקודה-לנקודה.

טבלה 5.6: *סיכום המאפיינים של תקשורת אינפרא-אדום נקודה-לנקודה*

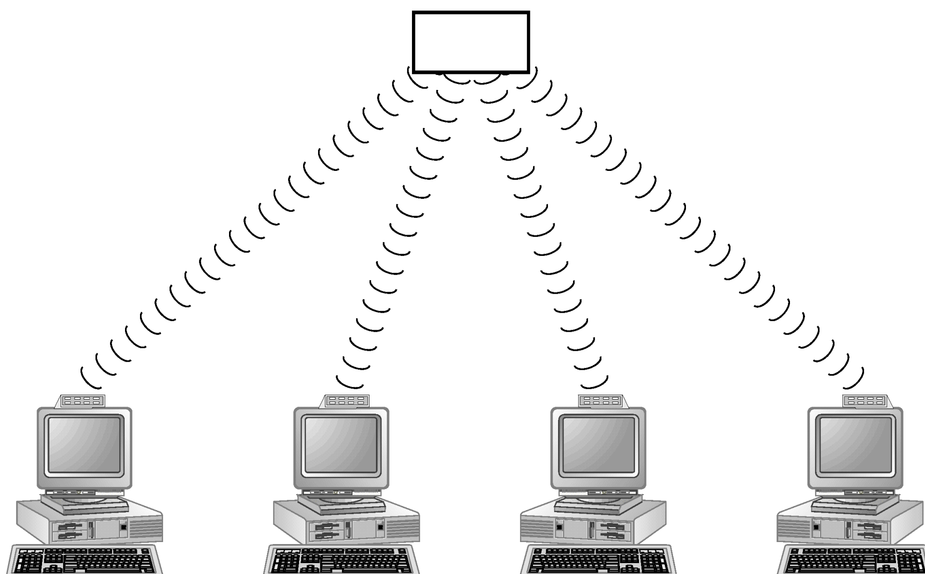
תדרים:	100GHz-1,000THz
טווח מירבי:	מוגבל לקו-ראייה. טכנולוגיות לייזר אחדות יכולות לשלוח אות על פני אלפי מטרים
מהירות שידור:	100Kbps-16Mbps
התקנה/תחזוקה:	בינונית. נדרש יישור מדויק של משדר ומקלט
הפרעות:	עמידה מאוד בפני הפרעות אלקטרומגנטיות, אך מקורות אור חזקים עלולים ליצור בעיות
עלות:	נעה בין זול (עבור טכנולוגיות LED) לבין יקר מאוד (עבור פתרונות לייזר)
אבטחה:	עמידה מאוד בפני ציתות בגלל דרישת קו-ראייה ומיקוד צר של אלומת האנרגיה

שידור אינפרא-אדום (Broadcast Infrared)

מערכות שידור אינפרא-אדום משתמשות בשיטה מסוימת **לפיזור** (dispersing) האות, כדי שיחידות רבות יוכלו לקלוט את השידור. בדוגמה המוצגת בתרשים 5.6, יחידות משדר בכל מחשב מכוונות את האות שלהן בכיוון הכללי של המשדר/מקלט שעל התקרה. יחידה זו, המכונה לעיתים **משדר אקטיבי** (active transmitter), מגבירה את האות ומשדרת אותו מחדש לאזור כולו. דרך חליפית לפיזור זה היא לשים חומר מחזיר (reflective) על התקרה שיכול להחזיר את האור האינפרא-אדום ממשדר בחזרה למטה לכל התחנות האחרות.



הערה: טלוויזיות ומערכות סטריאו רבות משתמשות בסוג זה של שידור. בדרך כלל ניתן להשתמש ביחידת השלט הרחוק מרוב המקומות בחדר. יחידות עם עוצמה חזקה יותר יכולות להחזיר (bounce) את האות שלהן מקירות או מחלונות.



תרשים 5.6: *מערכות תקשורת שידור אינפרא-אדום יכולות להחליף את החיווט של LAN*

מערכות המשתמשות בשידור אינפרא-אדום בדרך כלל קלות להתקנה ולהגדרה, מכיון שלא נדרש כוונון מדויק. החיסרון העיקרי של מערכות אלו הוא במהירות השידור הנמוכה. מכיון שאינן ממוקדות לאלומה צרה כמו מערכות נקודה-לנקודה, בדרך כלל הן לא מסוגלות לשדר במהירויות העולות על 1Mbps. למרות שהדבר מגביל את השימושיות שלהן ברוב סביבות רשת, הן יכולות להוות פתרון מתאים למצבים שבהם נדרשת ניידות ומהירות העברת הנתונים אינה קריטית.

בטבלה 5.7 תמצא סיכום המאפיינים של תקשורת שידור אינפרא-אדום.

טבלה 5.7: *סיכום המאפיינים של תקשורת שידור אינפרא-אדום*

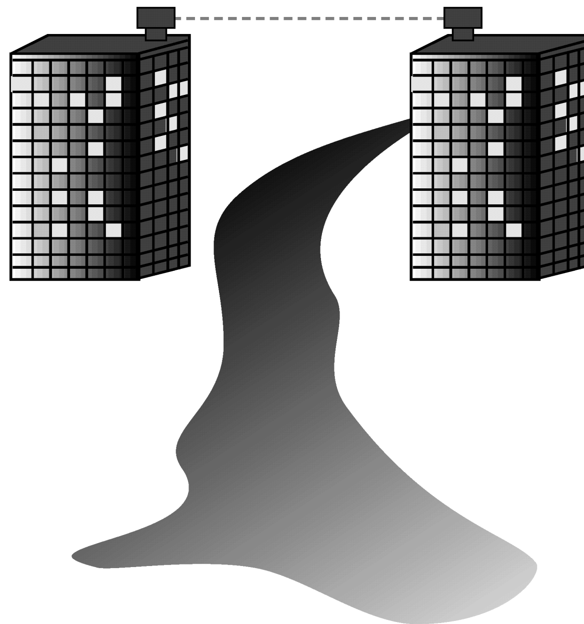
תדרים:	100GHz-1,000THz
טווח מירבי:	עשרות מטרים
מהירות שידור:	בדרך כלל 1Mbps או פחות
התקנה/תחזוקה:	קלה
הפרעות:	עמידה מאוד בפני הפרעות אלקטרומגנטיות, אך מקורות אור חזקים עלולים להפריע לאות
עלות:	זולה, אך יקרה יותר מרשת דומה המשתמשת בכבלים
אבטחה:	רגיש יותר מנקודה-לנקודה בגלל אזור שידור רחב. אך מוגבלת בדרך כלל לאזור מצומצם

יישומים של תווך אלחוטי

למרות שרשתות אלחוטיות בדרך כלל יקרות יותר מרשתות כבלים דומות, קיימות נסיבות רבות שבהן המאפיינים של רשתות אלו עשויים להתאים בדיוק לצרכים.

הרחבת הרשת המקומית

אחד המצבים שבהם תקשורת אלחוטית עשויה להיות אידיאלית היא כאשר יש שני בניינים הנמצאים בקרבה פיסית, ולא ניתן לחבר ביניהם כבל, בגלל מכשול כלשהו בין הבניינים כמו כביש מהיר, נהר או ואדי עמוק. במקרים אלה, ניתן להקים **גשר אלחוטי** (wireless bridge) בעזרת אחד האמצעים שתוארו בעמודים הקודמים (ראה תרשים 5.7). לחיבורים קצרי טווח, חיבור רדיו מסוג spread spectrum יכול לספק פתרון זול. אולם, פתרון מיקרוגל קרקעי או פתרון מבוסס לייזר (אינפרא-אדום) עשויים לספק את הרמה הגבוהה ביותר של מהירות שידור נתונים ואבטחה.



תרשים 5.7: *ניתן להקים גשר אלחוטי בעזרת תקשורת אינפרא-אדום (לייזר)*



רעיון מפתח

גשר אלחוטי יכול לשמש לחיבור בין שתי רשתות במצבים שלא ניתן להשתמש בו בכבלים.

ייתכנו מקרים שבהם פתרונות אלחוטיים יהיו זולים יותר בהשוואה לפתרונות כבלים הדורשים קווים חכורים מחברת הטלפונים. אם אתה זקוק לחיבור 10Mbps בין שני משרדים הנמצאים בקו-ראייה אחד מהשני, ההשקעה החד-פעמית בתווך אלחוטי עשויה להיות זולה יותר לטווח ארוך מאשר התעריפים החודשיים של קווים חכורים בין המשרדים.

כאשר אתה מעוניין להרחיב את הרשת שלך על פני אזור גיאוגרפי גדול יותר, האפשרויות האלחוטיות העומדות בפניך הן בעיקר רשתות מיקרוגל. מערכות מיקרוגל קרקעי המשתמשות בשורה של מגדלי ממסר, עשויות לספק את החיבור הדרוש. מעבר לכך, אתה נכנס לעולם היקר של מיקרוגל לוויני. אם אתה צריך לתקשר עם משרד באזור נידח כלשהו, לווין עשוי להיות האפשרות היחידה.

קשרי רדיו בהספק גבוה ובתדר יחיד עשויים אף הם להתאים בנסיבות מסוימות. ברמות ההספק ובתדרים המתאימים, ניתן להחזיר אותות רדיו מהאטמוספרה ולעבור מרחקים גדולים. מערכות רדיו אלו גם מספקות קישוריות **רב-נקודתית** (multipoint) יעילה, והן יכולות לאפשר למשתמשים גישה מרחוק לרשת מחוץ לגבולות בניין המשרדים. הדבר מספק גם הרחבת הגישה לרשת המקומית עבור משתמשים שנמצאים ברכב, באוויר או בים.

מחשוב נייד

בנסיבות מסוימות, תרצה להחליף לחלוטין את כבלי הרשת המקומית שלך. לדוגמה: משרד מכירות המעסיק עובדים המשתמשים בעיקר במחשבים ניידים שהם נושאים אל מחוץ למשרד. חברת משלוחים הרוצה שעובדיה יהיו ניידים בכל אזור המחסנים בלי להיות קשורים לשולחן העבודה. בתוך בית חולים, רופאים או אנשי צוות אחרים רוצים גישה לרשת מכל מקום בבניין.

הסוג המדויק של רשת מקומית אלחוטית המשמשת במצבים שונים אלה יהיה תלוי במצב, בעיקר בגורמים כגון דרישות רוחב פס, עלות והמרחק הדרוש. פתרונות רדיו מסוג spread spectrum יכולים לספק ניידות אמיתית. מערכות הספק נמוך בתדר יחיד עשויים אף הם לספק חלופה יעילה. בדוגמת משרד המכירות, אם המחשב הנייד של העובד יכול להיות מוצב במקום קבוע בעת העבודה, פתרון אינפרא-אדום נקודה-לנקודה יספק את מהירות השידור הגבוהה ביותר. מערכות מיקרוגל בהספק נמוך מתאימות גם הן בסביבות מסוימות.

מבט אל העתיד

טכנולוגיה אלחוטית ממשיכה להתפתח במהירות, וטכנולוגיות חדשות עשויות לספק שיטות נוספות לשבירת החיבור הפיסי. כיום רוב שירותי האיתור תומכים בדואר אלקטרוני ובשירותים אחרים באמצעות רשתות המבוססות-רדיו. נוצרו גם תקנים לשידור דיגיטלי על פני רשתות טלפון סלולרי. פרוטוקול Cellular Digital Packet Data (CDPD) עשוי לספק בקרוב מנגנון נוסף לחיבור רשת פשוט עבור משתמשים ניידים. יוזמות לווין גדולות אחדות נמצאות בשלבים שונים העשויים להביא לטבעות לוויינים

הסובבים את כדור הארץ ומרחיבים את רוחב הפס הקיים לתקשורת לווינית. ככל שאנשים מגלים את היתרונות של אמצעים אלחוטיים, העלויות נופלות ונוכל לראות טכנולוגיות נוספות מתהוות בעתיד.

סיכום

תווך אלחוטי יכול לספק חלופה לכבל הפיסי המוכר. טכנולוגיות אלחוט פועלות בתדרים אלקטרומגנטים שונים. ככל שהתדר גבוה יותר, כך ניתן לשדר יותר נתונים. אולם עם העלייה בתדרים, קטן מרחק השידור כתוצאה מהנחתת האות והפרעות שונות אחרות. עלויות הציוד וההפעלה עולות גם הן עם העלייה בתדרים.

טכנולוגיות אלחוטיות מתחלקות לשלושה סוגים עיקריים: רדיו, מיקרוגל, ואינפרא-אדום.

טכנולוגיות רדיו פועלות בתדר יחיד או במספר תדרים. **מערכות תדר יחיד** (single frequency) יכולות להתקיים בהספק נמוך לשימוש מקומי או בהספק גבוה יותר לשימוש במרחק גדול יותר. **מערכות spread spectrum** משדרות נתונים במספר תדרים, על ידי חלוקת הנתונים למנות ושידור מנות שונות בתדרים שונים, או על ידי דילוג מהיר בין תדרים. מערכות spread spectrum עמידות יותר בפני ציתות מאשר מערכות בתדר יחיד.

תקשורת מיקרוגל פועלת בתדרים גבוהים יותר אולם מחייבות ששני הצדדים של הקשר יהיו בקו-ראייה. **מערכות מיקרוגל קרקעי** (terrestrial) משתמשות באנטנות פרבוליות ליצירת קשר נקודה-לנקודה בין שני אתרים. ניתן להרחיב קשר זה על ידי שימוש במגדלי ממסר. מיקרוגל **לוויני** (satellite) יוצר גם הוא קשר נקודה-לנקודה, אולם הוא עושה זאת על ידי החזרת האות מלווין גיאוסינכרוני.

מערכות תקשורת אינפרא-אדום פועלות בתדרים גבוהים עוד יותר הקרובות לאור הנראה. מערכות אינפרא-אדום המשתמשות בדיודות פולטות אור (LED) יכולות לפעול בקצבי נתונים גבוהים במערכת **נקודה-לנקודה** (point-to-point), או לספק קצבי נתונים נמוכים יותר, אך ניידות גבוהה יותר במערכת **שידור** (broadcast). טכנולוגיות לייזר יכולות לשמש גם הן ליצירת קשר נקודה-לנקודה.

יישום נפוץ של חיבורים אלחוטיים הוא יצירת **גשר אלחוטי** (wireless bridge) בין שני בניינים במקום שלא ניתן, או לא רצוי, להעביר כבל פיסי. חיבור זה יכול להתבצע באמצעות מערכות תקשורת מיקרוגל קרקעיות או לייזר. יישום נוסף יהיה החלפת כל הכבלים של רשת מקומית רגילה. מערכות של רשתות מקומיות כוללות בדרך כלל מערכות רדיו spread spectrum, רדיו בהספק נמוך ובתדר יחיד, או באינפרא-אדום.

6

תמסורת נתונים - Data Transmission

לאחר שהחלטת באיזה סוג של **תווך רשת** (network media) תשתמש לחיבור הפיסי בין המחשבים, עליך לבחון כיצד תגרום לנתונים לעבור באותו תווך רשת. עד סוף פרק זה תדע:

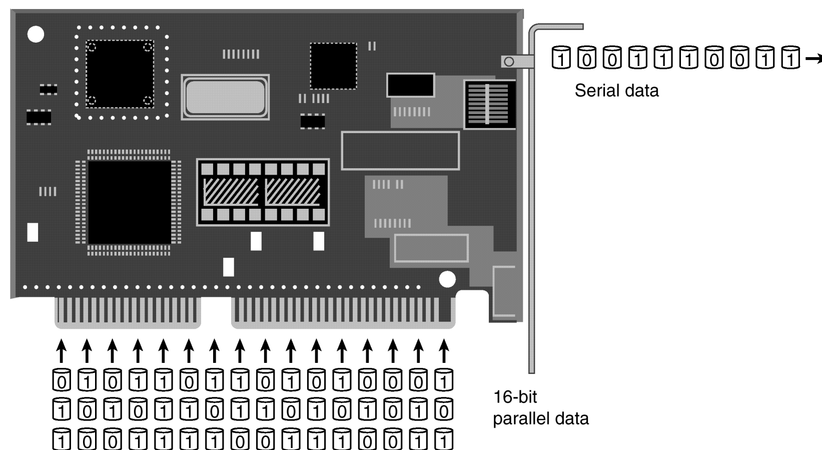
- ✯ להבין ולהגדיר כרטיסי ממשק רשת (NIC - Network Interface Card)
- ✯ להסביר את תפקידם של הדרייברים (מנהלי הֶתקֵן)
- ✯ לתאר את השיטות השונות לבקרה על זרימת הנתונים

כרטיסי ממשק רשת (NIC)

כאשר אתה רוצה לשלוח מידע ברשת, המחשב שלך משדר מידע זה בעזרת **כרטיס ממשק רשת - NIC** (Network Interface Card), המוכר גם כ**מתאם רשת** (network adapter), או **כרטיס רשת** (network card). בנוסף להכנה ושידור הנתונים, כרטיס ממשק הרשת גם מספק את החיבור הפיסי לתווך הרשת.

הנתונים זורמים בין רכיבים שונים במחשב, הם זורמים לאורך **אפיק** (bus או פס) נתונים. לדוגמה, כאשר המעבד זקוק לנתונים מהדיסק הקשיח, הנתונים עוברים מהדיסק הקשיח אל לוח האם של המחשב לאורך אפיק. ברוב המחשבים משתמשים באפיקים בעלי 32 סיביות, ואפיקים בעלי 64 סיביות נכנסים אט אט לתמונה.

אולם למרות שנתונים בתוך המחשב מתקדמים במקביל, המעבר בתווך הרשת הוא כמו נסיעה בנתיב אחד, בטור. כל הסיביות צריכות לעבור בטור. כפי שניתן לראות בתרשים 6.1, המשימה העיקרית של מתאם הרשת היא פתרון בעיית קליטת נתונים מאפיק בעל 16 או 32 נתיבים (מקבילי - Parallel), והעברתם לכביש חד-נתיבי (טורי - Serial) של הרשת. כרטיס ממשק הרשת (NIC) אורז את כל הנתונים ל**מנות נתונים** (data packets) ומשדר כל מנה באופן טורי בתווך הרשת (network media).



תרשים 6.1: *התפקיד העיקרי של כרטיס הרשת (NIC) הוא להמיר את הנתונים המקביליים (parallel) שמגיעים מאפיק הנתונים של המחשב, אל נתונים טוריים (serial) המיועדים להעברה בתווך הרשת*

כדי לשלוח את הנתונים בתווך הרשת, כרטיס ממשק הרשת חייב לכלול **משדר/מקלט** (transceiver) המתאים לתווך הרשת שבשימוש. לדוגמה, ברוב רשתות Ethernet, הכרטיס יכלול מחבר BNC לכבלי Thinnet או מחבר RJ-45 לכבלי UTP וימיר את הנתונים לאותות חשמליים. ברשת המשתמשת בכבל סיב-אופטי, כרטיס ממשק הרשת יכלול את המחברים המתאימים לכבל סיב-אופטי וימיר את הנתונים לאותות אור.

בנוסף לשידור הנתונים מהמחשב שלך אל הרשת, כרטיס ממשק הרשת גם מקבל את כל מנות הנתונים ששודרו בתווך הרשת וקובע אילו מנות מיועדות למחשב שלך. מנות אלו מומרות מזרימת הנתונים הטורית (serial) של הרשת לזרימה מקבילה (parallel) המתאימה למחשב.

הגדרות תצורה

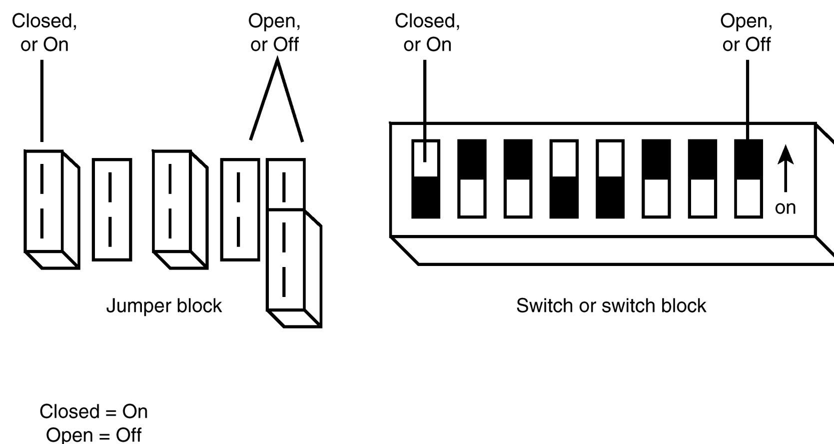
כאשר יש ברשותך כרטיס ממשק רשת המתאים למחשב שלך, עליך להגדירו לשימוש בתוך המחשב. בעולם האידיאלי, כל שיהיה עליך לעשות הוא לפתוח את המחשב, להכניס את כרטיס ממשק הרשת, לסגור את המחשב, ולהפעילו. כאשר המחשב מופעל, הכל אמור לעבוד מצוין, ותוכל מייד לתקשר עם הרשת. לרוע המזל, המציאות שונה מעט.

בשנים האחרונות, שיפרו היצרנים את הציוד שלהם והתקרבו לאידיאל שתואר קודם. מערכות ההפעלה Windows 9x של מיקרוסופט הציגה את תפישת **הכנס-הפעל** (Plug & Play). באופן תיאורטי, אם לוח האם של המחשב שלך, מערכת ההפעלה (Windows 9x/2000), וכרטיסי ההרחבה תומכים **כולם** בפונקציונליות הכנס-הפעל, תוכל להכניס את הכרטיס, להפעיל את המחשב והכל יפעל כשורה. כאשר המחשב עובר את תהליך ההפעלה הראשוני שלו Power-On Self-Test (הנקרא לעיתים POST), הוא יזהה את רכיבי הכנס-הפעל ויגדיר את ההתקנים אוטומטית. בדרך כלל הדבר פועל כאשר כל הרכיבים מתאימים לדרישות הכנס-הפעל. אם חלק מההתקנים אינם מסוג הכנס-הפעל, או אם הֶהתקֵן אינו תואם בדיוק לסטנדרטים של הכנס-הפעל, תצטרך להגדיר חלקים מסוימים במערכת שלך באופן ידני.

למערכות מחשבים מדור קודם, ולמערכות הפעלה אחרות מלבד Windows 9x/2000, תצטרך להגדיר ידנית את כרטיס ממשק הרשת לפני שיוכל לפעול עם המערכת. תצורת כרטיס רשת כרוכה בשינוי שלוש הגדרות (שלושה משאבים קריטיים):

- IRQ - Interrupt Request (בקשת פסיקה)
- Base I/O port (כתובת בסיס לקלט/פלט)
- Base memory address (כתובת בסיס בזיכרון)

לעיתים ניתן להגדיר הגדרות אלו בתוכנה, אולם ברוב המקרים, עליך לשנות **מגשר** (jumper) או **מתג DIP** (DIP switch), כפי שתוכל לראות בתרשים 6.2. מגשר למעשה הוא מחבר קטן המחבר שני פינים יחד ומשלים מעגל חשמלי. **מתג DIP** (Dual Inline Package switch) הוא התקן קטן עם מתגים מפלסטיק שניתן להפעיל או לנתק אותם בעזרת מברג קטן, או ציפורן.



תרשים 6.2: *רוב כרטיסי NIC מוגדרים באמצעות מגשר (jumper) או DIP switch*

IRQ - Interrupt Request (בקשת פסיקה)

בדרך כלל בתוך המחשב שלך יש רק שבב מיקרומעבד יחיד, המוכר גם כיחידת עיבוד מרכזית - CPU. קיימים התקנים רבים המחוברים לשבב זה באמצעות אפיק הנתונים, כמו למשל מקלדת, עכבר, כונני דיסק, מדפסות, כניסות טוריות, כרטיס קול וכרטיס ממשק רשת. מכיון שהתקנים רבים ניגשים אל המעבד דרך אפיק הנתונים, המעבד שמותקן במחשב צריך לדעת מתי התקן כלשהו זקוק לתשומת לב. לדוגמה, כאשר משתמש לוחץ על לחצן העכבר, צריכה להיות דרך כלשהי להודיע למעבד שהמשתמש יזם פעולת עכבר (לחיצה בלחצן). באופן דומה, אם כרטיס ממשק הרשת מקבל נתונים מהרשת, הוא זקוק למנגנון כלשהו שיודיע למעבד שיש לו נתונים לעבד.

בעולם החומרה של מחשבים, מנגנון זה נקרא **בקשת פסיקה** (interrupt request) או **IRQ**. למחשב שלך יש מספר קווי בקשת פסיקה (IRQ lines) מובנים המאפשרים לכל ההתקנים להודיע למעבד שהם זקוקים לשירות. מכיון שכל התקן חייב להשתמש בהגדרת IRQ ייחודית, עליך לקבוע אילו קווי IRQ זמינים לפני התקנת כרטיס ממשק הרשת. אם תכניס את הכרטיס ותציין קו IRQ שכבר בשימוש, לא תוכל לתקשר עם הרשת, ואולי אף תפריע לפעילות הרגילה של התקן אחר כלשהו.



טיפ: **במחשבים המשתמשים ב-**Microsoft DOS**,** Windows 3.x**, או** Windows 9x**, תוכל לכתוב את הפקודה** MSD.EXE **(זוהי פקודת** DOS**), כדי להריץ את** MSD **(**Microsoft System Diagnostics**), שהוא תוכנית אבחון המערכת של מיקרוסופט) ולגלות איזה קווי** IRQ **פנויים. ב-** Windows NT**, עליך להיכנס לתוכנית** Windows NT Diagnostics**, שנמצאת בקבוצת התוכניות או בתפריט** Administrative Tools**. לחילופין, ב-** Windows NT **תוכל לכתוב את הפקודה** WINMSD.EXE.

מנגנון בקשת הפסיקה קיים מראשית ימיו של המחשב האישי. מרבית בקשות הפסיקה הוקצו לשימוש משותף, כפי שניתן לראות בטבלה 6.1. כרטיסי ממשק הרשת הגיעו מאוחר יותר, ולכן יש להגדירם ל- IRQ שאינו בשימוש. מכיון שלרוב המחשבים לא מחוברת מדפסת שנייה (LPT2) או כרטיס קול, כרטיסי ממשק רשת מוגדרים במקרים רבים לשימוש עם IRQ5. IRQ3 משמש כחלופה נוספת, אם לא נעשה שימוש בכניסה טורית שנייה (com2). אם גם IRQ5 וגם IRQ3 אינם פנויים, מומלץ להתבונן בטבלה הבאה (טבלה 6.1) ולמצוא IRQ פנוי במערכת שלך.

טבלה 6.1: *הגדרות IRQ תקניות*

IRQ	שימוש אופייני
0	System timer.
1	מקלדת.
2	בקר IRQ משני, או מתאם וידאו.
3	לא בשימוש (אלא אם הוקצה עבור COM2, COM4 או עכבר אפיק).
4	כניסות טוריות COM1 ו- COM3.
5	לא בשימוש (אלא אם הוקצה עבור LPT2 או כרטיס קול).
6	בקר דיסקטים.
7	כניסה מקבילית LPT1.
8	שעון זמן אמיתי.
9	לא בשימוש, IRQ2 שהועבר לכאן, כרטיס קול, או בקר IRQ שלישי.
10	לא בשימוש, או בקר SCSI עיקרי.
11	לא בשימוש, או בקר SCSI משני.
12	עכבר PS/2.
13	Math coprocessor (מעבד מתמטי, אם מותקן).
14	בקר כונן דיסק קשיח עיקרי.
15	לא בשימוש, או בקר דיסק קשיח משני.



רעיון מפתח

עליך לדעת ש**כל** התקן חומרה זקוק ל- IRQ ייחודי ושקיימות הגדרות IRQ זמינות עבור כרטיסי NIC. מומלץ לשנן את הגדרות IRQ המוצגים בטבלה 6.1.

הערה: ברוב המחשבים היום ניתן לחבר שני דיסקים על כבל אחד לכרטיס IDE אחד.



הערה: ההקצאה המדויקת של IRQ2 ו-IRQ9 תהיה תלויה בחומרה שמותקנת במחשב. בימים הראשונים של מחשבים אישיים, הבקרה על הפסיקות היתה באמצעות שבב מעגל משולב - IC (Integrated Circuit) בעל שמונה פסיקות אפשריות בלבד (IRQ0-7). כאשר זה לא הספיק, נוסף שבב בקרת פסיקות נוסף לטיפול בפסיקות 8-15. מכיון שהמעבד ידע לקבל פסיקות משבב אחד בלבד, השני נוסף "תחת" הראשון במבנה הירכי. כאשר התקן המחובר לשבב השני היה זקוק לשירות, השבב השני היה מפעיל את IRQ2 שבשבב הראשון, והוא היה מעביר את הפסיקה למעבד. התקנים שהשתמשו קודם לכן ב-IRQ2 הועברו ל-IRQ9. כשנדרשו פסיקות נוספות, הוסיפו שבב שלישי (IRQ16-23) "תחת" השני, במקום IRQ9 בשבב השני (שהפעיל את IRQ2 בשבב הראשון, שהעביר את הפסיקה למעבד). הסדר זה ממשיך להתקיים ברוב המחשבים גם כיום.

כתובת בסיס לקלט/פלט - Base I/O Port

לאחר שהתקן השיג את תשומת ליבו של המעבד, עליו לשלוח אליו את הנתונים שלו. המעבד, בתורו צריך לשלוח נתונים בחזרה להתקן. מכיון שרוב ההתקנים משתתפים באותם אפיקי נתונים על לוח האם, צריכה להיות דרך כלשהי לקבוע מהו התקן היעד לנתונים הנשלחים מהמעבד. לצורך כך, לכל התקן מוקצית **כתובת בסיס לקלט/פלט** או **כניסה** - **base input/output (I/O) port** (לעיתים מכנים זאת דווקא "**יציאה**") המשמשת למעשה ככתובת שבה משתמש המעבד בעת תקשורת להתקן זה. כמו IRQ, כך, בדומה ל-IRQ, גם כתובת הבסיס לקלט/פלט (base I/O port) של כל התקן חייבת להיות ייחודית.

הכתובות נרשמות כמספרים הקסדצימליים שמבוטאים בתחום של 16 סיביות (300-30F). במקרים רבים הם נרשמים עם סיומת "h", כמו למשל "300h", או עם קידומת "0x", כמו למשל "0x300" כדי לציין שהמספר כתוב בבסיס הקסדצימלי. לכרטיסי ממשק רשת מוקצית בדרך כלל הכניסה 300h. ערכים נפוצים אחרים הם 280h או 310h. כאשר כתובות אלו אינן פנויות, חפש בטבלה 6.2 ערך שאינו מוקצה לחומרה המחוברת למחשב שלך.



טיפ: תוכל להשתמש שוב ב- MSD.EXE **או** Windows NT Diagnostics לקביעת כתובות (ports) המוקצות כבר במחשב שלך.

טבלה 6.2: *הקצאות base I/O port*

port (כניסה)	התקן	port (כניסה)	התקן
200	Game port	300	Network Interface Card
210		310	Network Interface Card
220		320	
230	Bus Mouse	330	
240		340	
250		350	
260		360	
270	LPT3	370	LPT2
280		380	
290		390	
2A0		3A0	
2B0		3B0	LPT1
2C0		3C0	EGA/VGA video adapter
2D0		3D0	CGA video adapter
2E0	COM4	3E0	COM3
2F0	COM2	3F0	Floppy-disk controller, COM1

כתובת בסיס זיכרון (Base memory address)

כדי להתמודד עם זרם הנתונים המגיע באפיק הנתונים המקבילי, יוצר כרטיס ממשק הרשת אזור **חציצה** (buffer) בזיכרון (RAM) של המחשב, שבו הנתונים מאוחסנים זמנית בעת המרתם לנתונים טוריים שיישלחו אל תווך הרשת. כתובת ההתחלה של אזור חציצה זה עבור כרטיס ממשק הרשת נקרא **כתובת בסיס זיכרון** (base memory address), או **כתובת זיכרון עליון** (upper memory address).

כמו IRQ ו- base I/O port, גם הכתובת הבסיסית לזיכרון - base memory address, חייבת להיות ייחודית לכל התקן. אולם, מכיון שרוב ההתקנים אינם משתמשים באזורי **זיכרון עליון** (upper memory), התחרות על הכתובות מוגבלת. כרטיסי ממשק רשת רבים משתמשים בכתובת D8000, ובדרך כלל אין צורך לשנות זאת.



הערה: מסיבות השמורות עימם, מקצרים יצרנים אחדים את הגדרת כתובת הבסיס בזיכרון על ידי הסרת הסיפרה האחרונה. לכן, NIC בעל כתובת זיכרון "D8000" תוגדר עם ערך "D800".

שיפור ביצועים

מעבר לנושאי הגדרות וסוגי אפיקים, קיימים גורמים רבים נוספים שיש לשקול לפני בחירת כרטיס ממשק רשת. הכרטיס חייב להמיר נתונים מהזרם המקבילי (parallel stream) של אפיק הנתונים במחשב לזרם הטורי (serial stream) של תווך הרשת. מכיון שאפיק הנתונים יכול לפעול במהירויות גבוהות הרבה יותר מאלו של תווך הרשת, כרטיס ממשק הרשת עלול להפוך לצוואר בקבוק (bottleneck) שיאט את פעילות המערכת כולה. רצוי שתהיה הזרימה המהירה ביותר האפשרית של נתונים דרך כרטיס ממשק הרשת (זרימת נתונים זו נקראת לעיתים **תפוקה, throughput**). ניתן לשפר את התפוקה באמצעות האפשרויות הבאות:

- **RAM buffering** (חציצת RAM). כרטיסי ממשק רשת רבים כוללים כיום שבבי RAM על הכרטיס עצמו. כאשר נתונים זורמים במהירות גבוהה מאפיק הנתונים של המחשב, ניתן לאחסן את המידע באופן זמני **בחוצץ RAM** (RAM buffer) בעת ההמתנה, עד שהשידור ייצא אל תווך הרשת. תהליך זה יכול להגביר מאוד את מהירות מתאם הרשת.
- **DMA - Direct Memory Access** (גישה ישירה לזיכרון). ללא DMA, המעבד שבמחשב מעורב בהעברה של כל הנתונים מכרטיס ממשק הרשת אל זיכרון המערכת. בקר DMA שבמחשב מוריד אחריות זו מהמעבד, ומטפל ישירות בהעברת הנתונים. אם כרטיס הרשת והמחשב שלך תומכים ב-DMA, בקר DMA יעביר נתונים ישירות מהחוצץ שבכרטיס הרשת אל זיכרון המערכת, כך תימנע מעורבות המעבד בתהליך זה, והמעבד יהיה פנוי לפעילויות אחרות.
- **Bus mastering** (ניהול אפיק). בדומה ל-DMA, בשיטת ניהול האפיק כרטיס ממשק הרשת משתלט על אפיק הנתונים של המחשב ומעביר נתונים ישירות אל זיכרון המערכת מבלי לערב בכך את המעבד. למרות שניתן להגביר כך את המהירות במידה רבה, כרטיסים מסוג זה יקרים וראוי לשקול את השימוש בהם.
- **Onboard microprocessor** (מעבד על כרטיס). כרטיסי ממשק רשת רבים מזרזים עוד יותר את זרימת הנתונים על ידי תוספת מעבד נפרד על כרטיס הרשת המטפל בהעברת הנתונים. כך מורידים עומס מהמעבד המרכזי של המחשב שאינו צריך לעבד את הנתונים הנכנסים מהרשת.
- **Shared memory** (זיכרון משותף). במקרים מסוימים כרטיס הרשת יכול להכיל זיכרון RAM משותף עם המחשב. מכיון שהמחשב מתייחס לזיכרון זה כאילו היה מותקן ישירות במחשב, המעבד יכול לקרוא ולכתוב נתונים ישירות אל הזיכרון המשותף. מכיון שהזיכרון המשותף כבר נמצא על כרטיס הרשת, הכרטיס יכול להעביר נתונים במהירות אל תווך הרשת וממנו.

כל השיטות יכולות לסייע בשיפור מהירות העברת הנתונים בין אפיק הנתונים של המחשב ותווך הרשת. כרטיסי ממשק רשת רבים משתמשים בשיפור אחד או יותר מאלה שתוארו כאן. מהירות ביצועי הכרטיס תגבר עם הוספת שיפורים, אולם גם מחיר הכרטיס יעלה. חשוב לבחור כרטיס ממשק רשת המתאים לרמת תקשורת הרשת שבה תשתמש. על השרתים להשתמש בכרטיסי רשת בעלי הביצועים הטובים ביותר

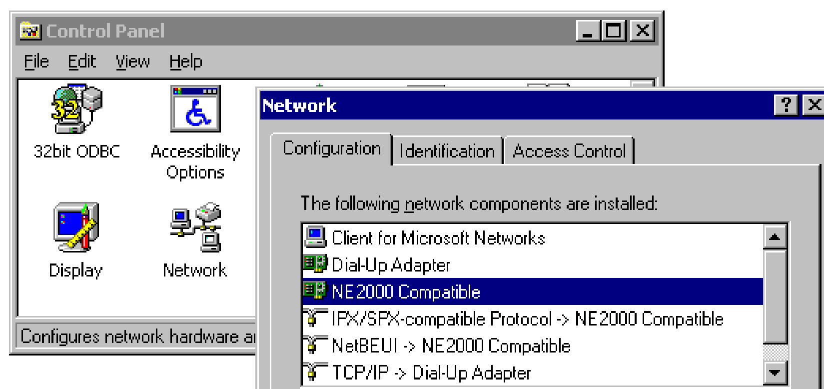
שתוכל להרשות לעצמך. אם מחשבי הלקוח לא ישתמשו ביישומים הפונים אל הרשת, כמעט כל כרטיס רשת יתאים. אולם, אם מחשבי הלקוח ישתמשו ברשת לעיתים קרובות, כדאי יהיה לצייד גם אותם בכרטיסי ממשק רשת בעלי ביצועים גבוהים.

מנהלי התקנים (Drivers)

לפני שתוכל להשתמש בכרטיסי ממשק הרשת, עליך להתקין **דרייבר** (driver - מנהל הֶתקֵן) לכרטיס. מכיון שיש מספר רב של יצרני כרטיסי רשת, קשה מאוד לספק מערכת ההפעלה לדעת את תצורת החומרה המדויקת של כל כרטיס רשת שנמצא בשוק.

במקום זאת, ספקי מערכות הפעלה פיתחו שיטת שימוש בדרייברים לתקשורת בין מערכת ההפעלה למתקן החומרה שבמחשב. למעשה, דרייבר הוא תוכנה קטנה המותקנת במערכת ההפעלה כדי לאפשר לה להשתמש בהתקן מסוים. לדוגמה, אם התקנת מדפסות במערכת, תזכור בוודאי התקנת דרייברים למדפסות אלו, כדי שתוכל להשתמש בהן.

התקנת דרייבר לכרטיס ממשק רשת היא תהליך פשוט בדרך כלל. מערכות הפעלה מודרניות כמו Windows 9x/NT/2000 כבר כוללות דרייברים עבור מיגוון רחב של כרטיסי ממשק רשת. בנוסף, רוב יצרני כרטיסי רשת מספקים תקליטור עם דרייברים למערכות הפעלה שונות. לכל מערכת הפעלה יש דרך שונה מעט להתקנת הדרייבר. עם זאת, מרבית מערכות ההפעלה מסתמכות על סוג כלשהו של ממשק גרפי לביצוע המשימה. תרשים 6.3 מציג התקנת דרייבר במערכת Windows.



תרשים 6.3: *Windows מספקת כלי התקנה גרפי להתקנת דרייברים*



הערה: למרות שרוב היצרנים מספקים דרייברים למערכות ההפעלה הנפוצות, לפני רכישת כרטיס ממשק רשת, מומלץ לוודא שקיים דרייבר עבור מערכת ההפעלה שלך. בנוסף, אם ספק מערכת ההפעלה מספק רשימת תאימות חומרה - HCL (Hardware Compatibility List), בחירת כרטיס רשת ודרייבר מהרשימה תספק רמה גבוהה ביותר של ודאות שהכרטיס יפעל כראוי במערכת.

בדרך כלל, בעת התקנת הדרייבר תתבקש לספק מידע תצורה, כמו למשל ה-IRQ של כרטיס ממשק הרשת.



רעיון מפתח

אם עליך לספק לדרייבר התוכנה שלך מידע תצורה, עליך להזין לו בדיוק את המידע שבו השתמשת בעת התקנת כרטיס ממשק הרשת. לדוגמה, אם הכרטיס מכוון להשתמש ב-IRQ5 ובכניסה 300h, עליך לוודא שגם הדרייבר מוגדר להשתמש בערכים אלה, אחרת הדרייבר לא יוכל לתקשר עם כרטיס הרשת ולא תוכל להשתמש ברשת.

שים לב שלאורך זמן, רוב היצרנים מעדכנים את הדרייברים שלהם כדי לשפר את הביצועים של כרטיסי ממשק הרשת. דרייברים מעודכנים אלה זמינים בדרך כלל מאתר Web של היצרן או של מיקרוסופט. אם יוצא לאור דרייבר מעודכן, ניתן להוריד מה-Web את הקובץ המעודכן ולהתקינו באותה דרך שבה הותקן הדרייבר המקורי. יכולת זו לשידרוג פשוט של דרייברים היא יתרון נוסף למנגנון השימוש בהם. אם התקשורת בין המחשב לכרטיס הרשת היתה מקודדת בתוך מערכת ההפעלה, לא היית יכול לשפר את ביצועי כרטיס הרשת עד ליציאת הגירסה הבאה של מערכת ההפעלה.

העברת נתונים אל הרשת (בקרת הגישה לתווך - MAC)

בנוסף להמרת נתונים מאפיק הנתונים של המחשב לתווך הרשת, מחליט כרטיס ממשק הרשת (NIC) **מתי** המחשב יכול להעביר נתונים אל תווך הרשת. אם שני מחשבים מעבירים נתונים באותו זמן, המנות שלהם **יתנגשו** (collide) והאות החשמלי של הנתונים יושחת עד כדי דעיכת הנתונים.

מניעת **התנגשויות** (collisions) אלו וארגון העברת הנתונים הינם התפקידים העיקריים של ההתקנים המתפקדים בתת-השכבה **בקרת גישה לתווך** (Media Access Control) של **שכבת קישור הנתונים** (Data Link Layer) במודל OSI. קיימות שלוש שיטות עיקריות למתן גישה לתווך הרשת:

- Contention (תחרות)
- Token Passing (העברת אסימון)
- Demand Priority (עדיפות דרישה)

Contention (תחרות)

אם יש לך מספר נקודות טלפון בביתך עבור קו טלפון אחד, חווית בוודאי בקרת גישה מבוססת **תחרות** (contention). בעיקרון כל אחד בבית מתחרה על גישה לקו טלפון זה.

במערכת מבוססת-תחרות "טהורה", כל מחשב יכול לשדר בכל רגע. הדבר דומה לכך שכל בני הבית ירימו את השפופרת ויתחילו לחייג. אם אין אף אחד אחר על הקו, החיוג יצליח. אם היה מישהו אחר על הקו, השיחה שלך לא תעבור, אך תפריע לשיחה

המתקיימת. ככל שאנשים יבצעו שיחות רבות יותר, יופעל עומס על המערכת עד כדי קריסה. באופן דומה, בעולם המחשבים, שיטת גישה המבוססת לחלוטין על תחרות לא תפעל כראוי. כדי להשליט מעט סדר במערכת, נעשה שימוש בשתי שיטות:

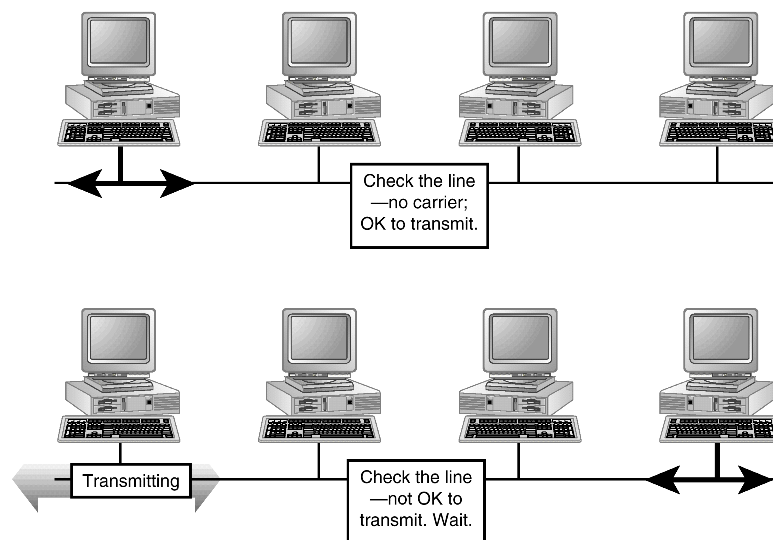
- ✯ CSMA/CD - Carrier-Sense Multiple Access with Collision Detection
- ✯ CSMA/CA- Carrier-Sense Multiple Access with Collision Avoidance

שתי השיטות מספקות אמצעי להגבלת מספר ההתנגשויות ברשת.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD)

נוהל CSMA/CD הוא למעשה השיטה שבה אתה משתמש בקו הטלפון הביתי שלך. בדרך כלל, אתה מרים את השפופרת ומקשיב לקבלת צליל חיוג. אם יש צליל חיוג אתה מחייג את המספר ומבצע את השיחה. כל עוד אתה משתמש בקו הטלפון, אף אחד אחר אינו יכול לחייג. אם אינך מקבל צליל חיוג, ואתה שומע מישהו אחר מדבר, עליך להמתין. אתה יכול להמשיך לבדוק, אולם כל עוד הקו בשימוש, אינך יכול לעשות דבר.

ייתכן מצב שאתה מרים את השפופרת באותו זמן שמישהו אחר עושה זאת, שומע צליל חיוג, ומתחיל לחייג באותו זמן (או כמעט באותו זמן) שהאדם האחר מחייג. מכיון ששניכם מחייגים בו-זמנית, המספרים המחויגים מפריעים זה לזה, ויצירת הקשר אינה מצליחה. בנקודה זו, אחד מכם יצטרך לוותר לחברו שיבצע את השיחה שלו וייאלץ להמתין לתורו.



***תרשים 6.4:** מחשבים ברשת המשתמשת ב-CSMA/CD בודקים את תווך הרשת לפני שהם שולחים נתונים כדי לבדוק אם הרשת בשימוש*

הדוגמה הקודמת מציגה כיצד פועלות רשתות מחשבים בשיטת CSMA/CD. כפי שניתן לראות בתרשים 6.4, למחשבים **רבים** יש **גישה** (access) לתווך הרשת. לפני שידור נתונים, כל מחשב **חש** (sense) אם הכבל פנוי או לא. אם כן, המחשב שולח את הנתונים שלו ואם לא, הוא ממתין עד שתווך הרשת פנוי. אם שני מחשבים או יותר משדרים נתונים בו-זמנית, הם **מזהים** (detection) את **ההתנגשות** (collision) של הנתונים שלהם עם הנתונים של מחשב אחר. בנקודה זו כל מחשב ממתין פרק זמן אקראי ואז מתחיל את התהליך מחדש. עם הפוגות אקראיות אלו בין שידורים חוזרים, הסיכויים שמספר מחשבים ישדרו בדיוק באותו זמן פוחתים במידה ניכרת.

למרות ששיטה זו נראית בלתי ישימה בסביבה מרושתת, CSMA/CD היא למעשה די מהירה ויוצרת את הבסיס לארכיטקטורת רשת Ethernet הנפוצה. היא אינה דורשת ציוד מתוחכם וניתן לממש אותה בעלות נמוכה. החסרונות של CSMA/CD כוללים:

- ✯ **יותר משתמשים - יותר התנגשויות**. עם הוספת משתמשים לרשת, יותר מחשבים מנסים לשדר את הנתונים שלהם. עם העלייה בשידור הנתונים, מספר ההתנגשויות גדל מאוד. בתעבורת רשת כבדה מאוד, שיטה זו עלולה להאט במידה משמעותית את מהירות הנתונים ברשת.
- ✯ **גישה לא שווה לתווך הרשת**. אם מחשב אחד משדר נתונים פעמים רבות, הוא יכול "להשתלט" על תווך הרשת, ולא לאפשר למחשבים אחרים הזדמנות לשדר.
- ✯ **אין אמצעים למתן עדיפויות לתעבורה.** כל המחשבים שווים בכך שכל תעבורת הרשת נראית שווה לכל המחשבים האחרים. אין כל דרך לציין שתעבורה משרת הרשת, למשל, צריכה לקבל עדיפות גבוהה יותר.
- ✯ **מגבלות מרחק.** בגלל ההנחתה (attenuation) של תווך הרשת, נראה שעם גידול אורך קווי הרשת, מחשבים בקצה אחד אינם יכולים "לחוש" האם מחשב בקצה האחר החל לשדר. רשתות CSMA/CD מוגבלות בדרך כלל ל-2500 מטר (1.5 מייל) או פחות.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

נוהל CSMA/CA דומה מאוד לנוהל CSMA/CD, אך עם הבדל קריטי אחד - מחשבים משדרים את כוונתם לשלוח נתונים לפני שהם משדרים אותם. תאר לעצמך שבביתך, לפני השימוש בטלפון, כל אחד היה צריך לצעוק כדי להודיע לכל האחרים על כוונתו לבצע שיחת טלפון. למרות שהדבר ימנע מקרים רבים שבהם שני אנשים מרימים את השפופרת בו-זמנית ומחייגים בו-זמנית, הבית יהיה רועש למדי.

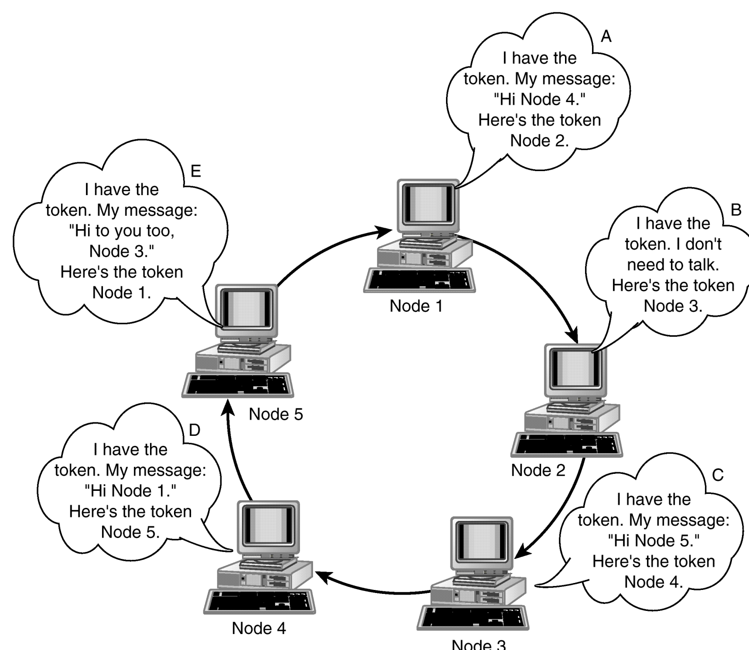
כמו ברשתות CSMA/CD, מחשב ברשת הפועלת בנוהל CSMA/CA (למשל רשת AppleTalk) בודק תחילה את תווך הרשת, כדי לברר אם הכבל בשימוש. אולם, שלא כמו ב-CSMA/CD, אם הכבל אינו בשימוש, המחשב מנסה למנוע התנגשויות על ידי שידור אות לרשת המציין שהוא מתכוון לשדר נתונים. לאחר שידור אות זה, הוא שולח את הנתונים עצמם. מחשבים אחרים שהתכוננו לשלוח נתונים ברשת ימתינו עם קבלת האות הראשון עד לאחר שידור הנתונים.

העיקר בשיטת גישה זו הוא, שכל אות כוונת שידור (signal of transmission intent) מופץ ברשת כולה. למרות שאותות כאלה עשויים למנוע התנגשויות נתונים רבות, השימוש המוגבר ברשת לשידור שלהם יאט במידה רבה את מהירות שידור הנתונים על פני הרשת. מסיבה זו, נוהל CSMA/CA אינו בשימוש נפוץ כמו CSMA/CD.

Token Passing (העברת אסימון)

תאר לעצמך סמינר קבוצתי בנושא מסוים. כשאתה מגיע, אתה מגלה שכל הכיסאות מסודרים במעגל. לאחר שכולם יושבים, המנחה מצהיר על תרגיל שבירת קרח, הוא מעביר חפץ כלשהו סביב המעגל. כאשר תקבל את החפץ, תוכל להציג את עצמך בפני הקבוצה ולומר לחברים משהו על עצמך. אף אחד אחר אינו יכול לדבר כאשר החפץ אצלך, ומותר לך לדבר במשך פרק זמן נתון. כאשר תסיים, תעביר את החפץ לאדם היושב לצידך. אם אין ברצונך לומר דבר, אתה יכול להעביר את החפץ מייד לבא בתור.

רשתות המשתמשות בשיטת גישה של העברת אסימון פועלות כך. כפי שמוצג בתרשים 6.5, מנת נתונים מיוחדת, **אסימון** (token), עוברת ברצף סביב מעגל הרשת. כאשר מחשב מקבל את האסימון, הוא יכול לשדר נתונים לכל מחשב אחר. בסיום, או אם אין לו מה לשדר, הוא מעביר את האסימון למחשב הבא. בגלל האופי המעגלי של השיטה, רשתות העברת אסימון ממומשות בדרך כלל **בטופולוגיית טבעת** (ring topology).



תרשים 6.5: *רשת המשתמשת בהעברת אסימון מספקת לכל המחשבים גישה שווה לאמצעי הרשת*

העוצמה והיתרון של גישה זו בכך שמחשבים יכולים לשדר רק כאשר האסימון אצלם, ולכן אין כל התנגשויות. גישה לתווך הרשת מובטחת כאשר האסימון "בידך". ברשתות בעלות נפח תעבורה גבוה, רשתות העברת אסימון יכולות לספק רמה גבוהה של ביצועים, מכיון שמחשבים אינם חסומים בהמתנה לפתרון התנגשויות. בנוסף, מכיון שניתן לקצוב את פרק הזמן שהאסימון יכול להימצא בכל מחשב, רשתות העברת אסימון יכולות להתאים לסביבות שבהן זמן הנתונים קריטי, כגון מפעלי ייצור אוטומטיים.

החיסרון העיקרי של רשתות העברת אסימון הוא, שהאסימון חייב תמיד לעבור בסבב ברשת. אם יש תעבורת רשת נמוכה מאוד ורק מחשב אחד רוצה לשדר, הוא עדיין חייב להמתין לתורו.

חיסרון נוסף הוא שתהליך העברת האסימון ברשת דורש ציוד מורכב ויקר יותר (כרטיסי ממשק רשת, רכזות, וכד') מאשר הציוד הנדרש עבור רשת מבוססת התנגשות.



טיפ: דרך נוספת לזכור מהן שיטות הגישה שדנו בהן כעת, היא לחשוב על נסיעה בצומת. רשתות מבוססות התנגשות דומות לכניסה לצומת ללא רמזור. אם אינך רואה אף אחד מתקרב לצומת, אתה יכול לפנות. השיטה פועלת היטב כאשר אין תנועה רבה. יחד עם זאת, אם מתקרב טור ארוך של מכוניות, אתה יכול להמתין זמן רב. העברת אסימון דומה לצומת שבו מותקן רמזור. לכל אחד מובטחת הזדמנות להיכנס לצומת, אולם אם יש אור אדום, עדיין תצטרך להמתין לאור הירוק, גם אם אין אף אחד אחר בסביבה.



הערה: ארכיטקטורות רשת רבות משתמשות בהעברת אסימון, כולל טבעת אסימון (Token Ring, תקן IEEE 802.5), אפיק אסימון (Token Bus, תקן IEEE 802.4) ו- FDDI. טבעת אסימון ו- FDDI יידונו בפירוט בפרק הבא.

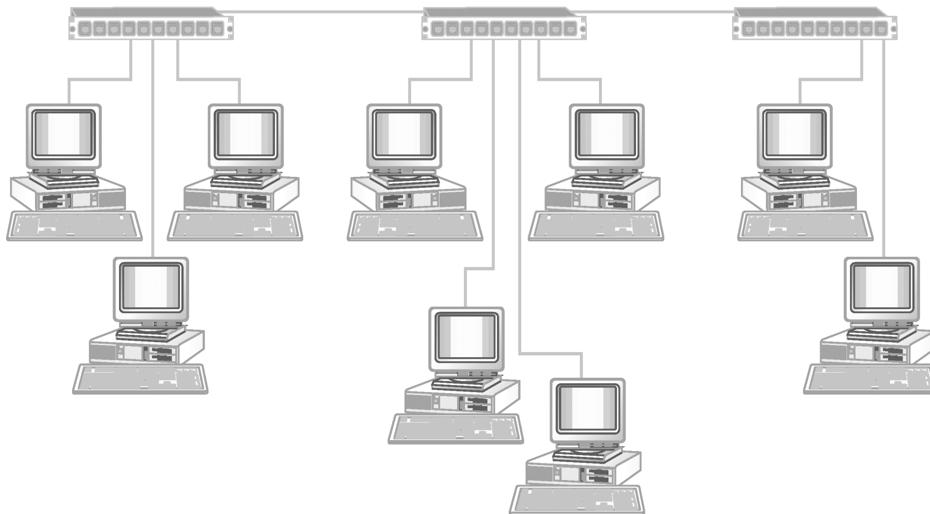
עדיפות דרישה - Demand Priority

ברשתות חדשות יותר המשתמשות בתקן 100VG-AnyLAN 100Mbps (המוכר גם כ- IEEE 802.12), רכזות חכמות פועלות ברשת **כוכב-אפיק** (Star Bus), כפי שמוצג בתרשים 6.6. הרכזות קובעות איזה מחשבים יכולים לשדר נתונים לרשת. מחשב שולח אות, הנקרא **דרישה** (demand), לרכזת כדי לציין שהוא רוצה לשדר. הרכזת מגיבה באישור שהמחשב יכול להתחיל לשדר מנות נתונים. הרכזת עוברת בין המחשבים שהגישו דרישה, ומאפשרת לכל אחד מהם לשדר מנה אחת לפי התור.

התנגשויות אינן מהוות כל קושי, מכיון שהרכזת (hub) מפקחת על הגישה לרשת. אם מספר מחשבים מגישים דרישות בו-זמנית, הרכזת תקבע אם אחד המחשבים מוגדר כבעל עדיפות גבוהה יותר מהאחר. אם כן, היא תאפשר למחשב המועדף לשדר נתונים ראשון. אם המחשבים בעלי עדיפות שווה, הרכזת תאפשר לכל מחשב לשדר מנה בכל פעם לפי התור.

נוהל עדיפות דרישה (demand priority) גם מייעל את השימוש בתווך הרשת. שלא כמו ברשתות העברת אסימון, מחשבים שאין להם נתונים לשדר אינם מעורבים כלל, עד שהם מבקשים שירות מהרכזת. בנוסף, מנות מועברות בין המחשב לרכזת ומהרכזת אל היעד, ואינן משודרות בכל הרשת כמו ברשתות CSMA/CD ו- CSMA/CA.

היעילות של גישה זו מושגת במחיר מסוים. החיסרון העיקרי של שיטת הדרישה הוא העלות הגבוהה של רכזות מיוחדות וציוד נוסף הנדרש להפעלת השיטה.



תרשים 6.6: עדיפות דרישה *משתמשת ברכזות חכמות לקביעה איזה מחשבים צריכים גישה לרשת*

השוואה בין שיטות גישה שונות

בעת רכישת כרטיס ממשק רשת, צריך לזכור שהכרטיס יצטרך לספק שיטת גישה לתווך המתאים לרשת שלך. רוב כרטיסי הרשת יזוהו ככרטיסי Ethernet או כרטיסי Token Ring. ההבדלים בין שיטות הגישה השונות מסוכמים בטבלה 6.3.

הסוג הנפוץ ביותר של רשת תקשורת מקומית הנמצא בשימוש כיום, הוא רשת Ethernet מבוססת contention (CSMA/CD). היא מהירה בסביבות בעלות תעבורה נמוכה, ודורשת רק תוכנה פשוטה וחומרה זולה. רשתות CSMA/CA נמצאות בעיקר בסביבות AppleTalk.

רשתות העברת אסימון נפוצות בסביבות עם תעבורת רשת כבדה, או העברת נתונים התלויים בזמן. רשתות העברת אסימון נחשבות כאמינות יותר, מכיון שמובטח שהנתונים ישודרו.

בדרך כלל מערכות עדיפות דרישה (demand priority) נמצאות ברשתות חדשות יותר, המשתמשות בארכיטקטורת 100VG-AnyLAN.

טבלה 6.3: *השוואה בין שיטות גישה שונות.*

שיטת גישה	יתרונות	חסרונות	ארכיטקטורות לדוגמה
Contention (תחרות) פופולרית ביותר בסביבת LAN	מהירה בתעבורה נמוכה זולה	איטית בתעבורה גבוהה אין הבטחה לגישה אין מנגנון עדיפויות	Ethernet (CSMA/CD) IEEE 802.3 LocalTalk (CSMA/CA)
Token passing (העברת אסימון) בדרך כלל בסביבת רשת עם עומס תנועה	מהירה בתעבורה גבוהה גישה מובטחת קריטית-בזמן	איטית בתעבורה נמוכה יקרה יותר	Token Ring IEEE 802.5 ARCnet ANSI 878.1 Token Bus IEEE 802.4 FDDI ANSI X3T9.5
Demand Priority (עדיפות דרישה) חדשה, בסביבת 100Mbps	מהירה גישה מובטחת אפשרות לקביעת עדיפויות	יקרה הרשת תלויה במרכזיה	Demand Priority 100VG-AnyLAN IEEE 802.12

סיכום

תהליך חיבור המחשב שלך לתווך הפיסי של הרשת כרוך בבחירת **כרטיס ממשק רשת - NIC** (network interface card) מתאים ובחירת תוכנת ה**דרייבר** (driver) המתאימה. כרטיס ממשק הרשת הנקרא גם **כרטיס מתאם רשת** (network adapter card), אשר ממיר נתונים המגיעים **מאפיק הנתונים** (data bus) המקבילי של המחשב לזרם טורי של סיביות שניתן לשדר בתווך הרשת. הכרטיס כולל גם **משדר/מקלט** (transceiver) המחבר פיסית את הכרטיס לתווך הרשת, ממיר את סיביות הנתונים לאותות חשמליים או אופטיים, ושולח אותם אל תווך הרשת. המשדר/מקלט גם קולט מידע מתווך הרשת ומעביר אותו לרכיבים האחרים של הכרטיס.

לאחר רכישת NIC, יש להגדירו כיאות לפני התקנתו במחשב. אם הכרטיס, לוח האם ומערכת ההפעלה המותקנת במחשב תומכים בארכיטקטורת **הכנס-הפעל** (plug & play), כל שיהיה עליך לעשות הוא לכבות את המחשב, להרכיב את הכרטיס במקומו, לסגור את המחשב ולהפעילו. כל התצורה תוגדר אוטומטית. אפשרות זו נתמכת על ידי מערכות ההפעלה Windows 9x/2000.

אם הכרטיס ומערכת ההפעלה אינם תומכים בהכנס-הפעל, תצטרך להגדיר ידנית את הכרטיס. הדבר כרוך בדרך כלל בהגדרת IRQ (interrupt request) וכניסת קלט/פלט (base I/O port). שתי הגדרות אלו מבוצעות באמצעות מתג DIP או **מגשר** (jumper). כל התקן המחובר למעבד של המחשב חייב להשתמש ב-IRQ ייחודי וכניסת קלט/פלט ייחודית. עבור כרטיסי ממשק רשת, יש להגדיר גם את כתובת הזיכרון הבסיסי (base memory address) של הכרטיס.

לאחר ביצוע ההגדרות המתאימות בכרטיס והתקנתו, תזדקק לדרייבר (device driver) כדי שהוא יוכל לפעול כהלכה. יש הגדרות אפשריות רבות לכרטיסי ממשק רשת, ולכן ספקי מערכות ההפעלה דורשים מיצרני כרטיסי ממשק רשת לספק דרייבר שיאפשר למערכת ההפעלה לתקשר עם הכרטיס. הדרייבר הוא תוכנה קצרה המותקנת בדרך כלל באמצעות ממשק גרפי.

לסיום הלימוד כיצד רשתות פועלות, עליך להבין כיצד כרטיס הרשת יודע מתי לשדר נתונים אל תווך הרשת. קיימות שלוש **שיטות גישה** (access methods) עיקריות בשימוש כיום והן: contention (תחרות), token passing (העברת אסימון), ו- demand priority (עדיפות דרישה).

למעשה, רשתות מבוססות תחרות, כמו Ethernet או AppleTalk, מאפשרות לכל מחשב לשדר בכל רגע. אם שני מחשבים או יותר משדרים באותו זמן מתרחשות **התנגשויות** (collisions), ויש לשדר את הנתונים מחדש. רשתות העברת אסימון, כגון **טבעת אסימון** (token ring), מונעות התנגשויות ומבטיחות גישה לתווך הרשת על ידי העברה רצופה של מנה הנקראת **אסימון** (token) ומחשבים יכולים לשדר רק כאשר האסימון נמצא אצלם. רשתות הפועלות בנוהל עדיפות דרישה המשתמשות בתקן החדש 100VG-AnyLAN מפקידות את כל בקרת הגישה בידי רכזות חכמות. מחשבים שולחים **דרישה** (demand) לשירות אל הרכזת, המאפשרת למחשב לשדר נתונים.

7

ארכיטקטורת רשת (שיטות גישור)

בפרקים קודמים של ספר זה, למדת אודות **תווך רשת** (network media), התפישות של טופולוגיות רשתות, שיטות גישה לרשת, וכיצד נתונים מועברים אל תווך הרשת. מצאת שסוגי תווך רשת פיסיים שונים יכולים לשמש רשתות מסוגים שונים, ומהי האינטראקציה בין כרטיסי ממשק רשת לתווך הרשת. נחשפת גם לרשתות **אפיק** (bus), **כוכב** (star) **וטבעת** (ring) וכיצד תעבורה זורמת ברשת. למדת גם אודות **מודל ייחוס OSI** (OSI Reference Model) וכיצד רשת אידיאלית אמורה לפעול.

כעת, נסתמך על מידע זה ונראה כיצד נושאים אלה משתלבים למה שנקרא **ארכיטקטורת רשת** (network architecture). הארכיטקטורה של רשת מתייחסת לא רק לטופולוגיה שלה, אלא גם לתווך הפיסי ולשיטת גישת הנתונים. למרות שמודל ייחוס OSI מתבסס על מודל רשת אידיאלית, ארכיטקטורות הרשת הנדונות בפרק זה יתייחסו לאופן הפעולה של רשתות בעולם האמיתי.

בפרק זה תלמד על ארכיטקטורות רשת עיקריות:

- Ethernet,
- Token Ring,
- ARCnet (Attached Resource Computer Network),
- FDDI (Fiber Distributed Data Interface),

ארכיטקטורות אלו מגדירות כיצד רשת פועלת בשכבה הפיסית ובשכבת קישור הנתונים של מודל ייחוס OSI.

Ethernet (מפרט IEEE 802.3)

בסוף שנות ה-60 וראשית שנות ה-70, ארגונים רבים ניסו למצוא דרכים לחיבור מספר מערכות מחשבים כדי לשתף משאבים. הניסיונות הראשוניים הובילו לפיתוח Ethernet (בשנת 1972) על ידי Robert Metcalfe ו- David Boggs, שני חוקרים במרכז המחקר - PARC (Palo Alto Research Center) של Xerox בפאלו אלטו, קליפורניה. הגירסה המסחרית הראשונה של Ethernet ששוחררה לשוק על ידי חברת זירוקס (Xerox) בשנת 1975, איפשרה למשתמשים לשדר נתונים בקצב הקרוב ל-3Mbps בין 100 מחשבים במרחקים המתקרבים לקילומטר אחד.

טכנולוגיה זו הוכחה כמצליחה כל כך, עד שהחברות זירוקס, אינטל, ודיגיטל פיתחו תקן חדש עבור Ethernet הפועל בקצב של 10Mbps. איגוד IEEE השתמש מאוחר יותר בתקן זה כבסיס למפרט הרשת 802.3 שלו, המגדיר כיצד רשתות Ethernet פועלות בשכבת קישור הנתונים ובשכבה הפיסית של מודל ייחוס OSI.

כיום, Ethernet התפתחה כארכיטקטורת הרשת הנפוצה ביותר לשימוש כללי. יתרונה בכך שהיא בדרך כלל אינה יקרה וקלה להתקנה ולהגדרה.

למעשה, קיימים סוגים שונים של רשתות המוגדרים תחת המטריה הקרויה Ethernet. כולם משתמשים בשיטה דומה לאריזת נתונים ב**מסגרות** (frames), ובאיתות פס בסיס להעברת נתונים, ורובם משתמשים ב-CSMA/CD (carrier-sense multiple-access with collision detection) לבקרת הגישה לתווך הרשת. רוב רשתות Ethernet יכולות להעביר נתונים במהירויות שמגיעות עד 10Mbps, אולם פותחו שני מפרטים חדשים יותר המאפשרים שידור ב- 100Mbps.

Ethernet מתממשת על בסיס כתובת ה"צרובה" ב-**ROM** (read only memory) של כרטיס ממשק הרשת (NIC), כדי לתקשר ברמת **המנה** (packet). הכתובות, הן של המחשב השולח את המידע והן של מחשב היעד, משולבות לתוך מסגרת הנתונים (data frame) הנשלחת אל תווך הרשת.

מפרטי Ethernet הנדונים בפרק זה מקובצים לשתי קטגוריות רחבות: 10Mbps ו- 100Mbps. הרשתות שעליהן תלמד הן:

- 10BaseT
- 10Base2
- 10Base5
- 10BaseF
- 100BaseT
- 100VG-AnyLAN



טיפ: הבנת מוסכמות IEEE למתן שמות לרשתות Ethernet תוכל להועיל לך. כפי שהוחלט במקור, היו לשם שלושה חלקים:

- ✯ מהירות העברת נתונים במגה-סיביות לשנייה (Mbps), מעוגלת למאה הקרובה ביותר.
- ✯ סוג תמסורת האות החשמלי (baseband לעומת broadband).
- ✯ מרחק מירבי שהרשת יכולה לכסות, במאות מטרים.

בדרך זו, הסוג 10Base5 ציין ארכיטקטורת רשת שתאפשר תמסורת פס בסיס של נתונים במהירות 10Mbps על פני מרחק של 500 מטרים. באופן דומה 10Base2 מאפשרת שידור על פני מרחק של עד 185 מטרים (מעוגל ל- 200 לצורך פשטות).

עם הזמן, מספר המרחק התגלה כלא מתאים לתיאור סוגי התווך החדשים, לכן Ethernet על פני זוג שזור (twisted pair) נקרא 10BaseT ועל פני סיבים אופטיים נקרא 10BaseF.

10Mbps

בראשית דרכה של Ethernet, היא הוגדרה כתקן 10Mbps. כיום נמצאות בשימוש ארבע תצורות נפוצות:

- ✯ 10Base5. Ethernet על כבל קואקסיאלי Thicknet (RG-11 או RG-8).
- ✯ 10Base2. Ethernet על כבל קואקסיאלי Thinnet (RG-58 A/U).
- ✯ 10BaseT. Ethernet על כבל זוג שזור לא-מסוכך (UTP), קטגוריות 3 עד 5.
- ✯ 10BaseF. Ethernet על כבל סיב-אופטי.

אלו משתמשות לבקרת גישת נתונים בתצורות מסגרת נתונים דומות וב- CSMA/CD.

10Base5

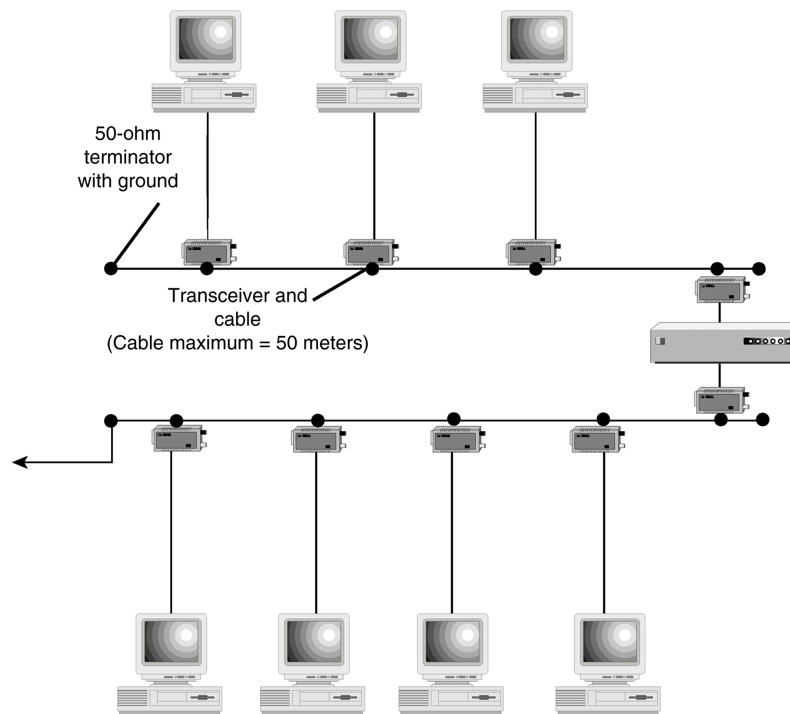
רשתות Ethernet המקוריות יצרו את הבסיס למפרט 10Base5 של IEEE. מפרט זה הגדיר רשת המשתמשת בכבל קואקסיאלי Thicknet לחיבור הדדי של עד 100 מחשבים ברשת אפיק עם מקטעים של עד 500 מטרים (1,640 רגל).

Thicknet משתמשת במשדר/מקלט המחובר לכבל הרשת באמצעות vampire tap. התקן זה מנקב את מעטה הכבל החיצוני ומקיים מגע ישיר עם המוליך הפנימי. **כבל סעף** (drop cable) מתחבר מהמשדר/מקלט אל **ממשק AUI** (Attachment Unit Interface), או אל כניסת DIX שעל כרטיס ממשק הרשת במחשב שלך. בסביבת 10Base5 טהורה, חייב להיות משדר/מקלט נפרד לכל חיבור רשת, כפי שמוצג בתרשים 7.1.



הערה: במפרט IEEE, החלק הנקרא כיום מחבר AUI או כניסת AUI, נקרא בעבר גם מחבר DIX על שם יוצרי הפרוטוקול: Xerox, Intel ו- Digital Equipment Corporation.

ל-10Base5 יש מספר דרישות מרחק ברורות. משדרים/מקלטים חייבים להיות במרחק של לפחות 2.5 מטרים (8 רגל) אחד מהשני, אחרת האות ייחלש. כל מקטע כבל יכול להיות באורך מירבי של 500 מטר. ניתן לחבר עד חמישה **מקטעים** (segment) בעזרת **מגברים** (repeaters), ליצירת רשת באורך כולל של 2,500 מטר. בנוסף, כבל סעף המחבר את המחשב והמשדר/מקלט אינו יכול להיות ארוך מ-50 מטר (164 רגל).



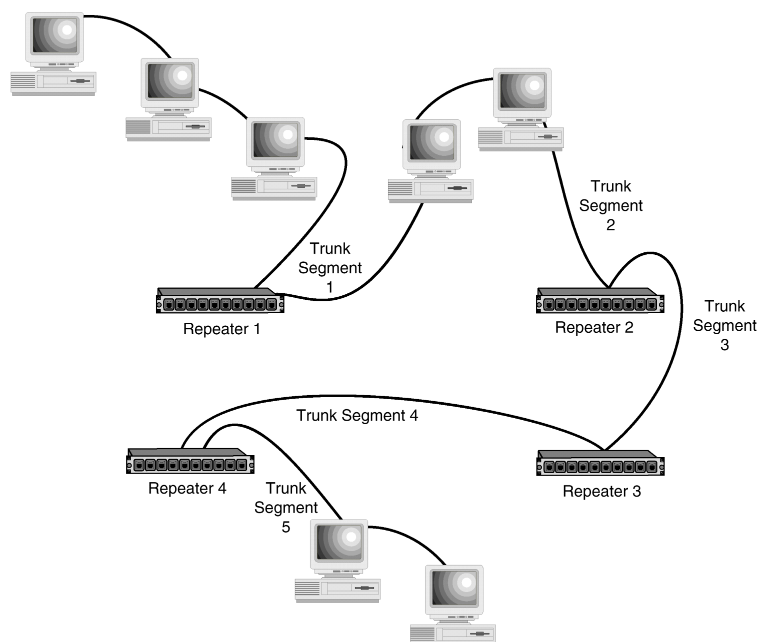
תרשים 7.1: *רשתות 10Base5 Ethernet משתמשות במשדרים/מקלטים מחוברים לכבל Thicknet*



טיפ: חשוב לדעת שאורכי כבלי הסעף (drop cables) **אינם** נכללים בחישוב האורך הכולל של הרשת. אורך **מקטע** (segment) של 500 מטר כולל רק את כבל Thicknet, המהווה את **אפיק השדרה** (backbone). על כן, אורכי כבלי הסעף אינם חשובים, לצורך זה (כבלי סעף מכונים לעיתים גם AUI cables, משום שהם מחברים את המקמ"ש (Transceiver) **לשקע** AUI אשר ב-NIC).

10Base5 גם מושפע מ**חוק 5-4-3** לתכנון רשתות Ethernet קואקסיאליות. כפי שמוצג בתרשים 7.2, לרשת 10Base5 יכולים להיות חמישה מקטעים המחוברים על ידי ארבעה מגברים (**רכזות, hubs**) עד לאורך רשת מירבי של 2,500 מטרים (8,200 רגל). אולם כתוצאה מדעיכת האות (attenuation), רק שלושה מהמקטעים יכולים להכיל חיבורי רשת. שני המקטעים האחרים יכולים לשמש לחיבור הרשת על פני מרחקים גדולים.

רשתות 10Base5 היו רשתות Ethernet המקוריות. אם הן נמצאות בשימוש כיום, הן משמשות בוודאי כאפיק השדרה של רשתות Ethernet אחרות. לדוגמה, תוכל למצוא Thicknet העובר בין בניינים עם משדר/מקלט בשני הקצוות, המחובר לרכֶּזת עם חיבורי 10Base2 היוצאים ממנה לרחבי הבניין.



תרשים 7.2: *חוק 3-4-5 קובע שרשתות Ethernet קואקסיאליות יכולות לכלול חמישה מקטעי רשת (Network Segment) המחוברים על ידי ארבעה מגברים כשרק שלושה מהמקטעים יכולים להכיל חיבורי רשת*

טבלה 7.1 מסכמת מידע אודות ארכיטקטורת רשת 10Base5.

טבלה 7.1: *סיכום מידע 10Base5*

סוג מידע	**מידע 10Base5**
יתרונות:	מרחקים ארוכים
חסרונות:	עלות גבוהה, קושי בהתקנה
טופולוגיה:	אפיק (bus)
סוג כבל:	50-ohm Thicknet
סוג מחבר:	מחבר AUI/DIX, Transceiver, Vampire tap
שיטת גישה לתווך רשת:	CSMA/CD
אורך מירבי למקטע:	500 מטר (1,640 רגל)
אורך מירבי כולל לרשת:	2,500 מטר (8,200 רגל)

טבלה 7.1: *סיכום מידע 10Base5 (המשך)*

סוג מידע	**מידע 10Base5**
מרחק מינימלי בין צמתים (nodes)	2.5 מטר (8 רגל)
מספר מירבי של מקטעים מחוברים :	5, כאשר רק 3 מאוכלסים
מספר מירבי של צמתים במקטע :	100
מספר מירבי של צמתים ברשת :	300
מהירות שידור :	10Mbps
מפרט IEEE :	802.3

10Base2

שלב ההתפתחות הבא של Ethernet כלל שימוש בכבל Thinnet. כבל Thinnet גמיש מאוד וקל להתקנה. שלא כמו ב-Thicknet, המשדר/מקלט (Transceiver) הוא חלק מכרטיס ממשק הרשת (NIC) ולכן כבל Thinnet מתחבר ישירות לכרטיס. כבל Thinnet משתמש במחבר BNC בטופולוגיית אפיק (bus) ודורש נגד סיום (terminator) בשני קצוות הכבל. אחד מנגדי הסיום צריך להיות מוארק - לדוגמה, באמצעות כבל הארקה או חוט המחובר מנגד הסיום לנקודת אדמה, למשל כמו בורג בשקע חשמלי.

מפרט IEEE עבור 10Base2 דורש שימוש בכבל RG-58A/U או בכבל RG58C/U. לכבל זה יש עקבה (impedance) של 50 אוהם וליבה מרכזית המורכבת ממספר סיבים.

> **רעיון מפתח**
>
> **זכור שהסוגים היחידים שצוינו על ידי IEEE הם RG-58A/U ו-RG-58C/U. RG-58U (או RG-58/U) אינו מקובל. באופן דומה, RG-59, כבל 75 אוהם המשמש טלוויזיה בכבלים, לא יפעל כראוי.**

בדומה ל-10Base5, רשתות 10Base2 מוגבלות על ידי חוק 5-4-3 לחמישה **מקטעים** (segments) באורך 185 מטר כל אחד, המחוברים על ידי ארבעה **מגברים** (repeaters), ורק שלושה מהמקטעים יכולים להכיל חיבורי רשת. בתוך כל מקטע של 185 מטר, ניתן לקשר חלקים קטנים יותר של כבל בעזרת **מחברי קנה** (barrel connectors), אולם כל מחבר קנה פוגע באיכות האות בכבל.

מכיון שרשתות 10Base2 מתממשות בעלות נמוכה יותר מאשר רשתות Thicknet, הן נכנסו לשימוש נרחב, ועדיין ניתן למצוא אותן במקומות רבים היום. יתרון העלות של רשתות 10Base2 הפך משמעותי פחות עם פיתוח רשתות 10BaseT הבנויות על תווך רשת זול עוד יותר - זוג שזור לא-מסוכך - UTP. פיתוח רשתות 10BaseT המשתמשות בטופולוגיית **כוכב** (star) גם מתגבר על השבירות הטבעית של טופולוגיית אפיק (bus) המשמשת ברשתות 10Base2.

טבלה 7.2 מסכמת מידע אודות ארכיטקטורת רשת 10Base2.

*טבלה **7.2**: סיכום מידע 10Base2*

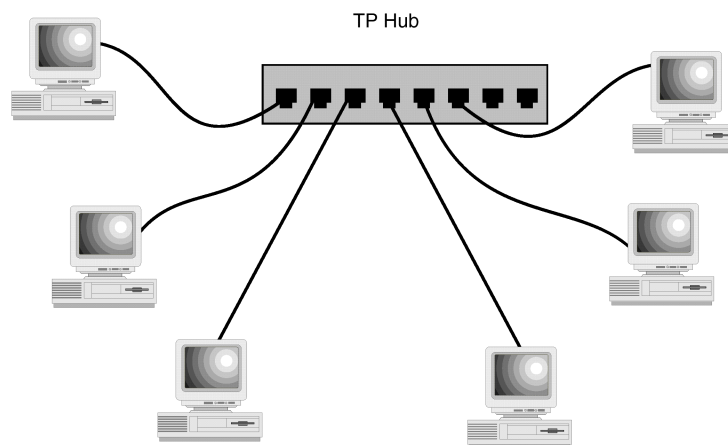
סוג מידע	מידע 10Base2
יתרונות:	קלה להתקנה, זולה יחסית
חסרונות:	קשה לאתר תקלות ברשת בטופולוגיית אפיק
טופולוגיה:	אפיק (bus)
סוג כבל:	RG-58C/U -ו RG-58A/U - 50-ohm Thinnet
סוג מחבר:	BNC
שיטת גישה לתווך רשת:	CSMA/CD
אורך מירבי למקטע:	185 מטר (607 רגל)
אורך מירבי כולל לרשת:	925 מטר (3,035 רגל)
מרחק מינימלי בין צמתים (nodes):	0.5 מטר (20 אינץ')
מספר מירבי של מקטעים מחוברים:	5, כאשר רק 3 מאוכלסים
מספר מירבי של צמתים במקטע:	30
מספר מירבי של צמתים ברשת:	90
מהירות שידור:	10Mbps
מפרט IEEE:	802.3

10BaseT

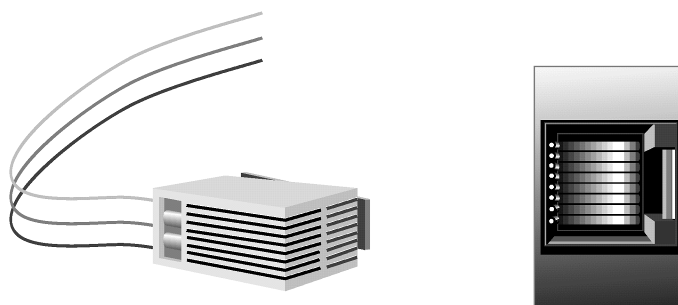
רשתות 10BaseT מבוססות על כבל UTP והן ללא ספק רשתות Ethernet הנפוצות ביותר בשימוש כיום. על ידי שימוש בטופולוגיית כוכב כפי שמוצג בתרשים 7.3, רשתות 10BaseT אינן חשופות לאותן בעיות איתור תקלות כמו 10Base2 ו- 10Base5. תווך UTP זול מאוד, וכך גם מרבית החומרה הנוספת הקשורה לרשתות 10BaseT, כמו למשל כרטיסי ממשק רשת (NIC) ורכזות (hub). בדומה ל- 10Base2, המשדר/מקלט (transciever) כלול בדרך כלל בכרטיס הרשת. כבלי UTP מתחברים ישירות לתקע RJ-45 שעל הכרטיס (ראה תרשים 7.4).



טיפ: מפרט IEEE עבור 10BaseT **מחייב** UTP. כאשר זוג שזור לא-מסוכך (STP) **אינו** חלק מהמפרט.



תרשים 7.3: *רשתות 10BaseT משתמשות בכבל UTP בטופולוגיית כוכב (star)*



תרשים 7.4: *כבלי UTP מתחברים לתקע RJ-45 על כרטיס ממשק רשת*

מכיון שהרכזות הפעילות ברשתות גדולות משמשות כמגברים (repeaters) להגברת עוצמת האות, רשתות 10BaseT אינן כפופות לחוק 3-4-5. תקן IEEE 802.3 מציין שניתן לחבר עד 1,024 מחשבים לרשת 10BaseT באמצעות מספר רכזות.

למרות שרשתות 10BaseT פועלות ביעילות עם כבל UTP מקטגוריות 3, 4 ו-5. רוב ההתקנות החדשות משתמשות ב-UTP בקטגוריה 5 (Category 5), מכיון שקטגוריה זו מתאימה גם לקיבולת העתידית של 100Mbps.



טיפ: זכור ש- Category 3 היא המינימום הנדרש עבור 10BaseT. **זכור גם, שכבלים העוברים בתקרה ובקירות של רוב הבניינים המודרניים חייבים להיות** plenum-rated.

החיסרון העיקרי של 10BaseT הוא המרחק הקצר יחסית שניתן לכסות עם UTP (100 מטרים). כדי להתגבר על כך, במקרים רבים ניתן למצוא 10BaseT היוצא מרכזות (hub) המחוברות ביניהן על פני מרחקים ארוכים בעזרת חיבור 10Base2 או חיבור 10BaseF (טופולוגיית star-bus).

טבלה 7.3 מסכמת מידע אודות ארכיטקטורת רשת 10BaseT.

טבלה 7.3: *סיכום מידע 10BaseT*

סוג מידע	**מידע 10BaseT**
יתרונות:	זולה מאוד, קלה לחיבור ולאיתור תקלות
חסרונות:	מרחק מוגבל
טופולוגיה:	כוכב (star)
סוג כבל:	זוג שזור לא-מסוכך - UTP (Categories 3-5)
סוג מחבר:	RJ-45
שיטת גישה לתווך רשת:	CSMA/CD
אורך מירבי למקטע:	100 מטר (328 רגל)
אורך מירבי כולל לרשת:	N/A
מרחק מינימלי בין צמתים (nodes):	2.5 מטר (8 רגל)
מספר מירבי של מקטעים מחוברים:	1,024
מספר מירבי של צמתים במקטע:	1
מספר מירבי של צמתים ברשת:	1,024
מהירות שידור:	10Mbps
מפרט IEEE:	802.3

10BaseF

מפרט IEEE עבור Ethernet במהירות 10Mbps הפועלת על כבלים סיב-אופטיים מוכר כ-10BaseF ומורכב למעשה משלוש קטגוריות משנה:

- ✩ **10BaseFL**. משמשת לקישור מחשבים בסביבת רשת מקומית (**L**an).
- ✩ **10BaseFP**. משמשת לקישור מחשבים עם רכזות פסיביות (**P**assive hubs, ללא מגברים) למרחקים מירביים של עד 500 מטרים.
- ✩ **10BaseFB**. כבל סיב-אופטי המשמש כאפיק שדרה (**B**ackbone) בין רכזות.

כל הסוגים משתמשים בטופולוגיית כוכב, כאשר הנתונים בהן מועברים באותות אור במקום אותות חשמליים. בדומה ל-10BaseT, ניתן לחבר יחד עד 1,024 צמתים בעזרת רכזות, אולם בגלל העלות הגבוהה של הכבלים והציוד, 10BaseF בדרך כלל אינה משמשת בסביבת רשתות מקומיות. ניתן למצוא אותה ברשת מקומית במצבים שבהם הפרעות אלקטרומגנטיות חזקות, או דרישות אבטחה גבוהות מצדיקות את השימוש בתווך רשת, אשר אינו חשוף להפרעות אלקטרומגנטיות. ברוב המקרים תמצא 10BaseF כאפיק שדרה המחבר בין רשתות 10BaseT שונות.

למרות שכבלי סיבים-אופטיים יכולים לפעול במהירויות גבוהות יותר מאשר 10Mbps המוגדרת במפרט 10BaseF, החיסרון העיקרי שלהם הוא העלות הגבוהה מאוד והקושי בהתקנה.

טבלה 7.4 מסכמת מידע אודות ארכיטקטורת רשת 10BaseF.

טבלה 7.4: *סיכום מידע 10BaseF*

סוג מידע	**מידע 10BaseF**
יתרונות:	מרחקים ארוכים
חסרונות:	יקרה מאוד, קשה להתקנה
טופולוגיה:	כוכב (star)
סוג כבל:	סיבים אופטיים
סוג מחבר:	מיוחד
שיטת גישה לתווך רשת:	CSMA/CD
אורך מירבי למקטע:	2,000 מטר (6,561 רגל)
אורך מירבי כולל לרשת:	N/A
מרחק מינימלי בין צמתים (nodes):	N/A
מספר מירבי של מקטעים מחוברים:	1,024
מספר מירבי של צמתים במקטע:	1
מספר מירבי של צמתים ברשת:	1,024
מהירות שידור:	10Mbps
מפרט IEEE:	802.3

100Mbps

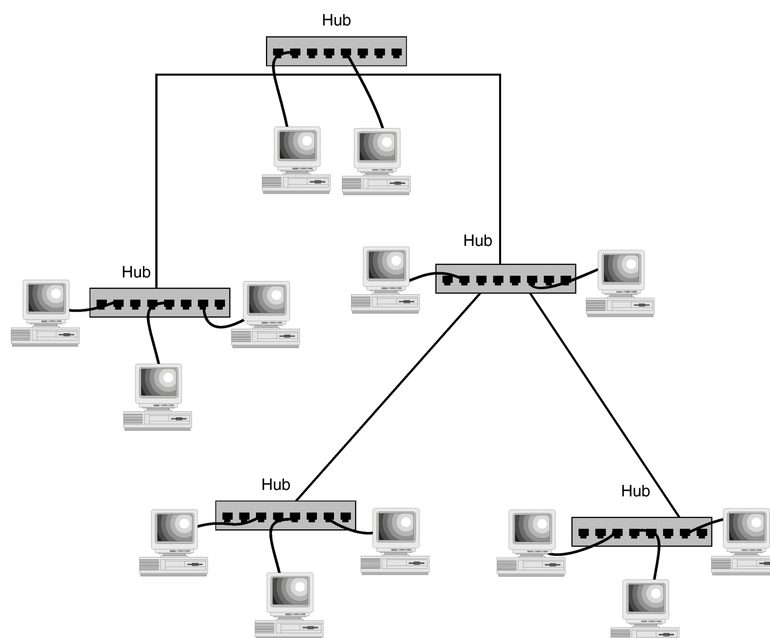
כשעלה הצורך במהירות רשת גבוהה יותר, יצרו הספקים שני תקנים מתחרים עבור קצבי שידור של 100Mbps ב-Ethernet: 100VG-AnyLAN ו-100BaseT. 100BaseT מתחלק לשלוש קטגוריות: 100BaseTX, 100BaseT4 ו-100BaseFX.

שני התקנים יידונו לעומק בהמשך, אולם קודם נבדוק מספר נקודות השוואה:

- 100VG-AnyLAN ו-100BaseT דורשים שניהם שהמשתמשים **ישדרגו** את כרטיסי ממשק הרשת שלהם (NIC).
- למרות ששני התקנים משתמשים בכבל UTP, 100BaseTX דורש כבל Category 5 ואילו 100VG-AnyLAN ו- 100BaseT4 יכולים להשתמש בכבל קטגוריה 3, 4 או 5 כל עוד יש בו ארבעה זוגות חוטים. בכל המקרים, חלק מהמשתמשים יצטרכו לשדרג חלק מהכבלים המותקנים אצלם.
- עם 100BaseTX ועם 100BaseT4 התקשורת מוגבלת לטווח של 100 מטר. רשתות 100VG-AnyLAN המשתמשות בכבל UTP קטגוריה 3 או 4 מוגבלות גם הן לטווח של 100 מטר. אולם, 100VG-AnyLAN יכולה להגיע למרחק של 150 מטר על ידי שימוש ב-UTP קטגוריה 5.
- הן 100VG-AnyLAN והן 100BaseFX יכולות להשתמש בכבלי סיבים-אופטיים לשידור על פני מרחקים של עד 2,000 מטר.
- ספקים יצרו כרטיסי ממשק רשת עבור שני הֶתקנים המאפשרים למנהלי הרשת לעבור בקלות מרשתות 10BaseT אל רשת זו. משתמשים יכולים להתקין את כרטיס ממשק הרשת החדש ולהמשיך להשתמש בו עם 10BaseT, עד שיהיו מוכנים לעבור לרשת במהירות גבוהה יותר.
- רשתות 100BaseT יכולות לשדר מסגרות מסוג Ethernet בלבד, ואילו רשתות 100VG-AnyLAN יכולות להעביר הן Ethernet והן מנות Token Ring, וכך ניתן לשלבן בקלות בשתי הארכיטקטורות.
- 100BaseT מוגדרת במפרט 802.3 של IEEE, ואילו 100VG-AnyLAN מוגדרת תחת מפרט 802.12 החדש של IEEE.

100BaseT

100BaseT, הנקראת גם **Fast Ethernet** או **100BaseX**, היא למעשה תוצר של המאמצים להגברת הקיבולת של רשתות 10BaseT. רשת זו פותחה במקור על ידי Grand Junction Networks, 3Com, Intel ואחרים. היא מתאימה את תקן 802.3 לתמיכה בקצבי העברת נתונים של 100Mbps בעיקר על פני כבלי Category 5 UTP. כדי לעשות זאת, רשתות 100BaseT משתמשות בכבלים קצרים יותר ומקשרות מספר רכזות, כפי שמוצג בתרשים 7.5.



תרשים 7.5: *רשתות 100BaseT משתמשות בטופולוגיית כוכב בדומה לרשתות 10BaseT*

תקן 100BaseT מגדיר למעשה שלושה סוגי כבלים:

- ✰ **100BaseT4**. ארבעה זוגות UTP קטגוריות 3, 4 או 5.
- ✰ **100BaseTX**. שני זוגות UTP קטגוריה 5.
- ✰ **100BaseFX**. כבל סיב-אופטי עם שני סיבים (strands).

גורם חשוב אחד אודות רשתות 100BaseTX הוא שהן **דורשות** כבל קטגוריה 5 (Category 5). רשתות 10BaseT רבות עדיין פועלות על כבלי UTP קטגוריה 3 עבור קול, אשר מותקנים במרבית מערכות הטלפון. יהיה צורך לשדרג כבל זה לפני שהרשת תוכל לעבור ל-100BaseTX.

100BaseT4 יכולה לתמוך ב-100Mbps על UTP קטגוריה 3, 4 או 5. אולם, היא דורשת שכל ארבעת הזוגות השזורים בכבל יהיו פנויים. מכיון ש-10BaseT דורשת רק שני זוגות חוטים, כיום קיימות התקנות בהן שני זוגות חוטים משמשים לנתונים וזוג אחר משמש לטלפון. במקרה זה יהיה צורך להתקין כבל UTP נוסף, שבו כל ארבעת הזוגות פנויים לפני שניתן יהיה להפעיל את 100BaseT4.

למרות שקיימים שלושה תקני כבלים, תקן 100BaseTX הפך לנפוץ ביותר, ובדרך כלל אנשים מתכוונים לתקן זה כאשר הם אומרים **100BaseT** או **Fast Ethernet**.

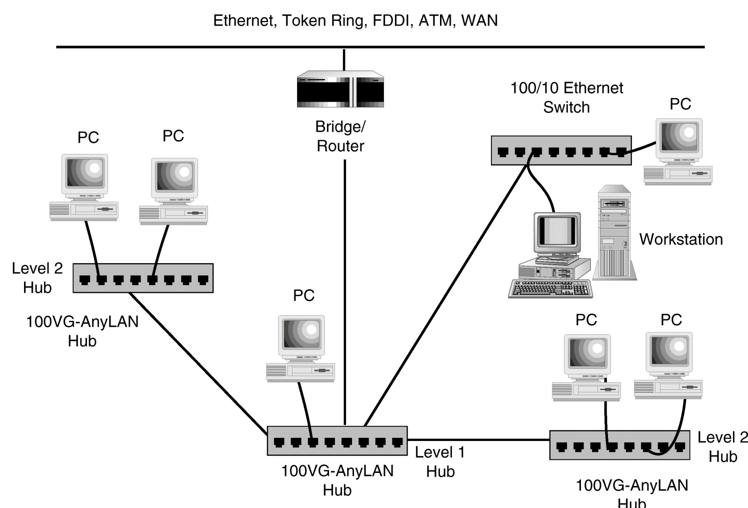
טבלה 7.5 מסכמת מידע אודות ארכיטקטורת רשת 100BaseT.

טבלה 7.5: סיכום מידע 100BaseT

סוג מידע	**מידע 100BaseT**
יתרונות:	מהירה, קלה לחיבור ולאיתור תקלות
חסרונות:	מרחק מוגבל, חומרה יקרה
טופולוגיה:	כוכב (star)
סוג כבל:	UTP קטגוריה 5 - 100BaseTX UTP קטגוריה 3, 4, 5 - 100BaseT4 כבל סיב-אופטי - 100BaseFX
סוג מחבר:	RJ-45
שיטת גישה לתווך רשת:	CSMA/CD
אורך מירבי למקטע:	100 מטר (328 רגל) - 100BaseTX, 100BaseT4 2,000 מטר (6,561 רגל) - 100BaseFX
אורך מירבי כולל לרשת:	N/A
מרחק מינימלי בין צמתים (nodes):	2,5 מטר (8 רגל)
מספר מירבי של מקטעים מחוברים:	1,024
מספר מירבי של צמתים במקטע:	1
מספר מירבי של צמתים ברשת:	1,024
מהירות שידור:	100Mbps
מפרט IEEE:	802.3

100VG-AnyLAN (מפרט IEEE 802.12)

תקן 100VG-AnyLAN פותח במקור על ידי Hewlett-Packard ו-AT&T. הוא משתמש בשיטת **עדיפות דרישה** (demand priority) לגישה לנתונים, ולא ב-CSMA/CD. במצב זה, רכזות חכמות מקבלות **דרישות** (demands) לשירות ממחשבים, ומאפשרות לאותם מחשבים לשדר למחשב היעד הרצוי. רשתות 100VG-AnyLAN משתמשות בטופולוגיית כוכב בדומה ל-10BaseT עם סדרה של רכזות **המקושרות במידרוג** (interlinked cascading), כפי שמוצג בתרשים 7.6. רכזת השורש המרכזית "root" מחוברת למספר רכזות, וכל אחת מהן יכולה להיות מחוברת לרכזות אחרות.



תרשים 7.6: *רכזות מחוברות ביניהן ברשת 100VG-AnyLAN ליצירת טופולוגיית כוכב.*

רשת 100VG-AnyLAN מתוכננת לפעול עם כל UTP **"דרגת קול"** ("voice grade") וניתן להשתמש בה על הרבה התקנות 10BaseT UTP קיימות מקטגוריה 3 או יותר. המגבלה היחידה היא ש- 100VG-AnyLAN זקוקה לכל ארבעת הזוגות השזורים בכבל UTP, ואילו 10BaseT זקוקה רק לשני זוגות (אחד לשידור ואחד לקליטה). קיימות התקנות כיום שבהן שני זוגות חוטים משמשים לנתונים וזוג אחר משמש לטלפון. במקרה זה יהיה צורך לשדרג את הכבל כך שכל ארבעת הזוגות יהיו פנויים להעברת נתונים לפני שניתן יהיה להפעיל 100VG-AnyLAN.



הערה: רשת 100VG-AnyLAN נקראת **לעיתים גם**: 100BaseVG, 100VG או AnyLAN.

עם עדיפות דרישה, רשת 100VG-AnyLAN מציעה מספר יתרונות ביצועים ברורים. מכיון שהרכזות מספקות את בקרת הגישה, מנות נתונים אינן משודרות ברחבי הרשת. הנתונים מנותבים דרך הרכזת (או הרכזות) מהמקור אל היעד. יש לכך יתרון נוסף ברמה גבוהה יותר של פרטיות, מכיון שלא כל המחשבים מקבלים את מנות הנתונים. תכונה נוספת היא שדרישות שירות נכנסות מסודרות על ידי הרכזות לפי סדר עדיפויות, ופריטים הזקוקים לשידור רגיש לזמן יכולים לקבל עדיפות גבוהה יותר.

יתרון נוסף של רשת 100VG-AnyLAN הוא שהיא אינה מוגבלת לשימוש ב- Ethernet. על ידי שימוש בדרייברים המתאימים לכרטיס ממשק הרשת, ניתן להגדיר את 100VG-AnyLAN לשימוש עם מסגרות Token Ring במקום מסגרות Ethernet, וכך ניתן לשלבה לתוך רשת Token Ring קיימת. על ידי שימוש בהֶתקן **מגשר** (bridge) וסוג המסגרת המתאים, רשת 100VG-AnyLAN יכולה להתקיים במקביל ולהחליף נתונים עם רשת Ethernet או עם רשת Token Ring.

כמו 10BaseT, גם ל-100VG-AnyLAN יש מרחק מירבי של 100 מטרים בין רכזת למחשב על פני כבלי UTP קטגוריה 3. שלא כמו ארכיטקטורות UTP אחרות, ברשתות 100VG-AnyLAN עם UTP קטגוריה 5, ניתן להגדיל מרחק זה ל-150 מטר. 100VG-AnyLAN מוגדר גם לשימוש עם כבלי סיבים-אופטיים במרחק עד 2,000 מטר.

טבלה 7.6 מסכמת מידע אודות ארכיטקטורת רשת 100VG-AnyLAN.

טבלה 7.6: *סיכום מידע 100VG-AnyLAN*

סוג מידע	**מידע 100VG-AnyLAN**
יתרונות:	מהירה, קלה לחיבור, קלה לאיתור תקלות, ניתן להשתמש בה עם מנות Ethernet ו- Token Ring. אפשרות לקביעת סדר עדיפויות
חסרונות:	מרחק מוגבל (UTP), חומרה יקרה
טופולוגיה:	כוכב (star)
סוג כבל:	UTP קטגוריות 3-5, זוג שזור מסוכך (STP), סיבים אופטיים
סוג מחבר:	RJ-45
שיטת גישה לתווך רשת:	**עדיפות דרישה** (demand priority)
אורך מירבי למקטע:	100 מטר (328 רגל) בשימוש ב-UTP קטגוריה 3 או STP 150 מטר (492 רגל) בשימוש ב-UTP קטגוריה 5 2,000 מטר (6,561 רגל) בשימוש בסיבים אופטיים
אורך מירבי כולל לרשת:	לא רלוונטי
מרחק מינימלי בין צמתים (nodes):	2.5 מטר (8 רגל)
מספר מירבי של מקטעים מחוברים:	1,024
מספר מירבי של צמתים במקטע:	1
מספר מירבי של צמתים ברשת:	1,024
מהירות שידור:	100Mbps
מפרט IEEE:	802.12

סוגי מסגרות Ethernet

לפני שתחקור ארכיטקטורות אחרות, עליך להכיר היבט אחד נוסף של Ethernet. ללא קשר לארכיטקטורת Ethernet שבשימוש, הנתונים ייארזו על ידי דרייבר הרשת וכרטיס ממשק הרשת ל**מסגרת** (frame) ויישלחו אל תווך הרשת.

קיימים ארבעה סוגי מסגרות שונים :

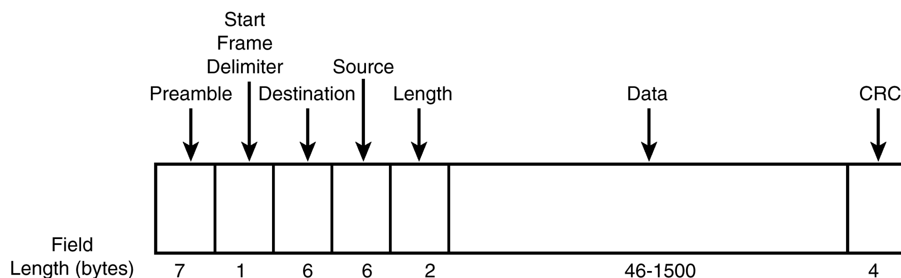
- ✯ **Ethernet 802.3**. משמש בעיקר ברשתות Novell NetWare 2.x, 3.x.
- ✯ **Ethernet 802.2**. משמש ברשתות Novel NetWare 4.x כברירת מחדל.
- ✯ **Ethernet SNAP**. משמש ברשתות AppleTalk אחדות.
- ✯ **Ethernet II**. משמש ברשתות TCP/IP.

כל סוגי המסגרות משתמשות במנה בגודל שבין 46 לבין 1,518 בתים, ויכולות לפעול עם ארכיטקטורות הרשת שתוארו לעיל. באופן כללי, הרשת שלך תשתמש רק בסוג אחד של מסגרות, אולם ייתכן מצב שמחשבים מסוימים, כגון שרתים, ישתמשו במספר סוגי מסגרות כדי לתקשר עם מקטעים שונים של הרשת. כדי שתתקיים תקשורת בין שני מחשבים המחוברים לרשת Ethernet, שניהם חייבים להשתמש באותו סוג מסגרת.

Ethernet 802.3

Ethernet 802.3 נמצאת בעיקר ברשתות נובל Netware גרסאות 3.x ומטה. סוג זה מוכר גם כ-**Raw Ethernet** (איטרנט גולמי). סוג מסגרת זה פותח לפני סיום הגדרת מפרט 802.3 של IEEE עבור Ethernet. לכן הוא אינו תואם לחלוטין את מפרט IEEE 802.3 ואינו פועל בכל סביבות Ethernet. כיום הוא נמצא בעיקר ברשתות Novell NetWare מגירסה 2.2 ו- 3.x.

כפי שמוצג בתרשים 7.7, מסגרת נתונים מסוג Ethernet 802.3 מתחילה עם שדה הקדמה (preamble) ושדה התחלה SFD (Start Frame Delimiter) בן בית אחד המציין את תחילת המסגרת. כתובות היעד והמקור באות אחר כך, ואחריהן שדה עבור אורך הנתונים והנתונים עצמם. המנה מסתיימת בבדיקת CRC (Cyclical Redundancy Check) המבטיחה שהנתונים לא ניזוקו בהעברה.



תרשים 7.7: *מסגרות Ethernet 802.3 מכילות מידע כתובות ואת אורך הנתונים*

Ethernet 802.2

Ethernet 802.2 נמצאת בעיקר ברשתות נובל Netware גרסאות 3.12 ו-4.x. מסגרות 802.2 מתאימות לחלוטין לתקן IEEE 802.3, והן משמשות סוג ברירת המחדל עבור רשתות Novell NetWare בגרסאות 3.12 ו-4.x. מסגרות Ethernet 802.2 מכילות שדות דומים ל-Ethernet 802.3, בתוספת שלושה שדות מסוג Logical Link Control (LLC).



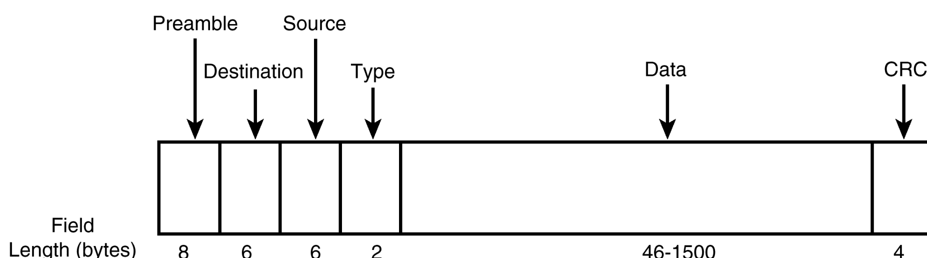
הערה: כן, קראת סעיף זה נכון. מסגרות Ethernet 802.3 **אינן תואמות את תקן** Ethernet 802.3 **של** IEEE, **ואילו מסגרות** Ethernet 802.2 **כן תואמות תקן זה.**

Ethernet SNAP

Ethernet SNAP נמצאת בעיקר ברשת Apple Talk. מסגרות Ethernet SNAP (SubNetwork Address Protocol) מציעות שיפורים לסוג מסגרת 802.2, כולל תוספת של שדה **סוג** (type), המציין איזה פרוטוקול רשת נמצא בשימוש בחלק הנתונים של המסגרת. מסגרות Ethernet SNAP משמשות בעיקר ברשתות AppleTalk Phase II.

Ethernet II

Ethernet II נמצאת בעיקר ברשת TCP/IP. רשתות TCP/IP ורשתות המשתמשות במספר פרוטוקולי רשת משתמשות בדרך כלל במסגרות Ethernet II. כפי שמוצג בתרשים 7.8, מסגרות אלו שונות ממסגרות 802.3 בכך שהן משלבות את ההקדמה ואת שדות SFD, וכוללות שדה סוג פרוטוקול במקום שבו מסגרות Ethernet 802.3 מכילות שדה אורך.

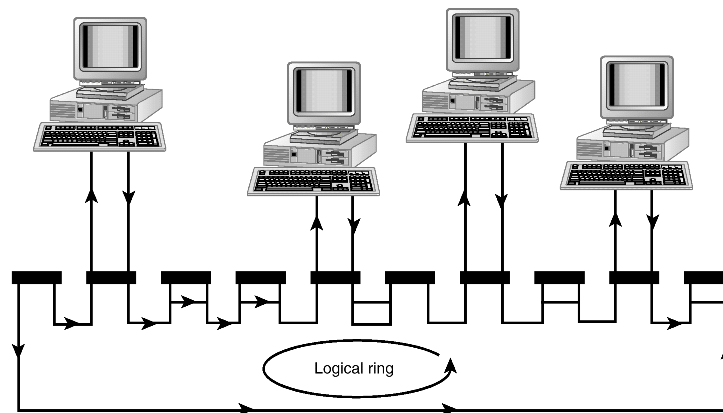


תרשים 7.8: *מסגרות Ethernet II כוללות שדה סוג המציין איזה פרוטוקול רשת נמצא בשימוש*

Token Ring (מפרט IEEE 802.5)

באמצע שנות ה-80, פיתחה יבמ ארכיטקטורת רשת Token Ring כדי לספק למשתמשים רשת מהירה ואמינה. רשת Token Ring, שהוכרזה מאוחר יותר כתקן IEEE 802.5, מחווטת פיסית בטופולוגיית כוכב, כמו רשתות 10BaseT Ethernet. אולם, כפי שניתן לראות בתרשים 7.9, הרשת היא **טבעת לוגית** (logical ring), כלומר הרכזת מחווטת כך שהאות עובר בטבעת.

רשתות Token Ring משתמשות בשיטת גישה של העברת אסימון (token-passing) כדי להבטיח שלכל מחשב ברשת יש הזדמנות לשדר נתונים. מסגרת נתונים קטנה המכונה **אסימון** (token) מועברת סביב הטבעת. כל מחשב ברשת מקבל את האסימון **משכנו הפעיל הקודם הקרוב ביותר - NAUN** (nearest active upstream neighbor). אם האסימון פנוי ולמחשב יש נתונים לשדר, הוא מחבר את הנתונים לאסימון ושולח אותו הלאה **לשכנו הפעיל הבא הקרוב ביותר - NADN** (nearest active downstream neighbor). כל מחשב מקבל את האסימון, קובע כי האסימון בשימוש, וחוזר על השידור של האסימון עם הנתונים, בדיוק כפי שהתקבלו, הלאה אל שכנו (NADN).



תרשים 7.9: *רשתות Token Ring מחווטות בכוכב פיסי, אולם מממשות טבעת לוגית*

כאשר הנתונים מגיעים אל מחשב היעד, הוא מעתיק את הנתונים ומעביר אותם לשכבות פרוטוקול גבוהות יותר להמשך העיבוד. מחשב היעד משנה שתי סיביות במנת הנתונים ומעביר את מנת הנתונים חזרה אל טבעת הרשת. כאשר האסימון והנתונים חוזרים למחשב המקור, הוא מוודא שהנתונים הועברו בהצלחה (על ידי הבחנה בשתי סיביות המתג ששונו) ואז משחרר את האסימון ומעבירו ל-NADN.

למרות שתהליך זה נראה מסורבל, הוא מאפשר העברה מהירה של נתונים. בדרך כלל המחשבים אינם צריכים לשדר נתונים פעם נוספת, מכיון שאין התנגשויות. כשעולה התעבורה ברשת האסימון ממשיך לעבור בין המחשבים, ומאפשר לכל מחשב לשדר נתונים.

רשתות Token Ring של יבמ פעלו בתחילה במהירות של 4Mbps. שיפורים מאוחרים יותר הגבירו את המהירות ל-16Mbps. מסגרות נתונים של Token Ring יכולות להיות באורך 4,000 עד 17,800 בתים, ביחס לגודל מסגרת מירבי של 1,500 בתים במסגרת נתונים של Ethernet.

בדומה לרשתות Ethernet, כל מחשב ברשת Token Ring משתמש בכתובת הצרובה בכרטיס ממשק הרשת שלו.



רעיון מפתח

זכור שרשתות Token Ring משתמשות במסגרת נתונים (data frame) **גדולה** יותר מאשר Ethernet. הדבר מאפשר העברה מהירה יותר של כמויות נתונים גדולות.

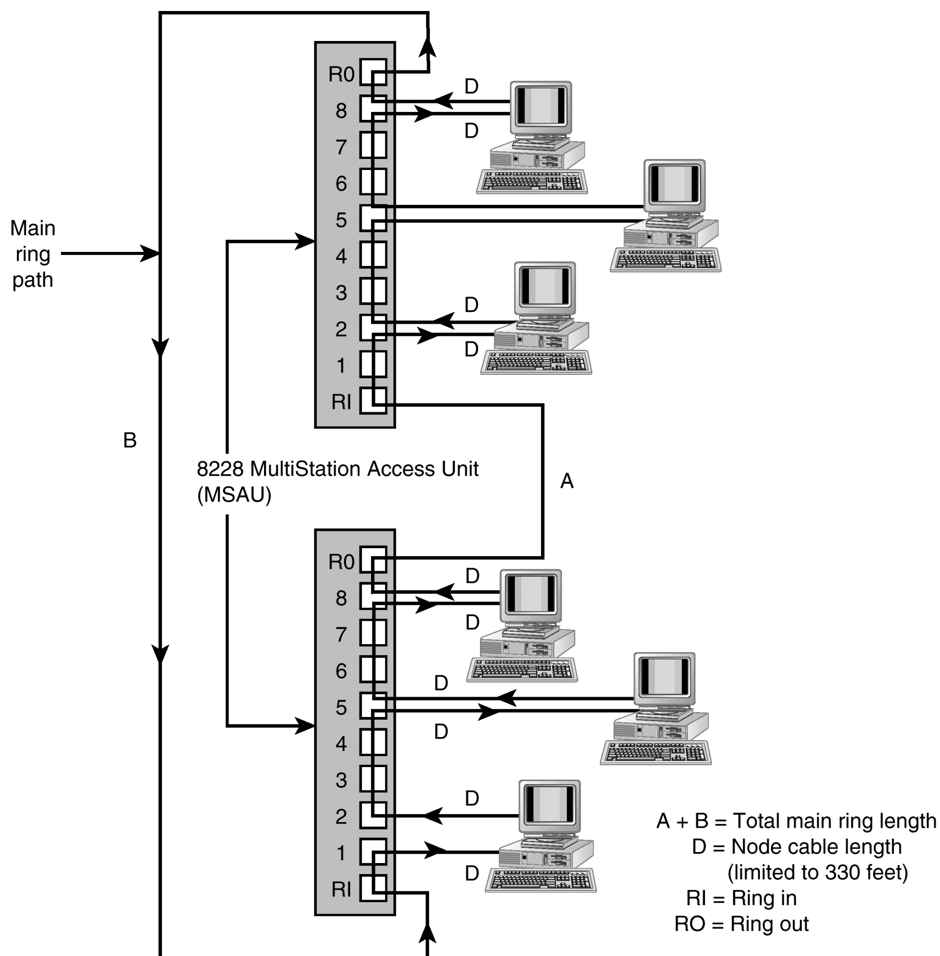
רכזות Token Ring

ברשת Token Ring כל רכזת נקראת MAU (Multistation Access Unit, יחידת גישה לתחנות רבות) ומחווטת כטבעת לוגית, כפי שהוצג קודם בתרשים 7.9.



הערה: רכזת Token Ring נקראת גם **MSAU** (MultiStation Access Unit) או **SMAU** (Smart Multistation Access Unit).

ל-MAU אופיינית של יבמ יש עשר כניסות לחיבורים, שמונה משמשות לחיבורים למחשבים. שתי הכניסות האחרות הן RI (Ring In, טבעת פנימה) ו-RO (Ring Out, טבעת החוצה), אשר מאפשרות לקשר בין יחידות MAU של Token Ring. תרשים 7.10 מראה כיצד יחוברו שתי יחידות MAU, כדי לספק גישה לעד 16 תחנות עבודה.



תרשים 7.10: *יחידות MAU (רכזות) של Token Ring מחוברות באופן שיוצר טבעת לוגית*

אם נדרשות רכזות נוספות, כל MAU יוסף כך שהטבעת הלוגית תישמר. מפרט יבמ עבור Token Ring קובע שניתן לחבר עד 33 רכזות בצורה זו. למרות שיחידות MAU המקוריות של Token Ring יכלו להכיל רק 8 חיבורי רשת, יבמ וספקים אחרים מייצרים כיום רכזות עם 16 כניסות ויותר.

כבלים ברשת Token Ring

רשתות Token Ring יכולות להשתמש בכבלי UTP או STP. בשנת 1984, יבמ פיתחה מערכת כבלים מקיפה שהגדירה סוגי כבלים, מחברים, וכל יתר הרכיבים הדרושים לרישות מחשבים. כש- Token Ring הוצגה היא השתמשה במערכת כבלים של יבמ.

מערכת הכבלים של יבמ מחלקת כבלים לתשעה סוגים שונים המוגדרים על סמך תקני AWG (American Wire Gauge) הקובעים קוטר חוטים. מספרי AWG מוקצים ביחס הפוך לקוטר, כלומר מספרי AWG גדולים מציינים קוטר קטן. עובי חוט טלפון רגיל הוא 22AWG, עובי כבל קואקסיאלי Thicknet הוא 12AWG, וכבל קואקסיאלי Thinnet הוא 20AWG. כבל 26AWG יהיה דק יותר מחוט טלפון רגיל.



הערה: אל תבלבל בין סוגי הכבלים של IBM עבור ארכיטקטורת Token Ring לבין קטגוריות UTP שהוגדרו לפי תקן שנכתב על ידי EIA/TIA.

סוגי הכבלים של יבמ:

- **Type 1**. כבל STP עם שני זוגות שזורים של חוט 22AWG עם ליבה מלאה (solid core) העטופים במעטה קלוע (braided) ומעטפת (casing). זהו **הכבל האופייני** המשמש בין מחשבים ויחידות MAU.
- **Type 2**. כבל STP עם שני זוגות שזורים של חוט 22AWG עם ליבה מלאה לנתונים וארבעה זוגות שזורים של חוט 26AWG לקול. משמש במצבים בהם רוצים להעביר קול ונתונים בכבל יחיד.
- **Type 3**. כבל UTP לקול עם ארבעה זוגות שזורים של חוט 22AWG או 24AWG. משמש כחלופה זולה יותר ל- Type 1, אולם אינו יכול להעביר יותר מ-4Mbps.
- **Type 4**. לא מוגדר.
- **Type 5**. כבל סיב-אופטי המשמש בעיקר לחיבור יחידות MAU על פני מרחקים ארוכים.
- **Type 6**. כבל STP עם שני זוגות שזורים של חוט 26AWG עם ליבת סיבים דקה (stranded core) העטופים במעטה קלוע ומעטפת. דומה ל- Type 1, אולם ליבת הסיבים הדקה מאפשרת גמישות רבה יותר, אך גם מגבילה את המרחק לשני שלישים מזה של Type 1. כבל זה משמש בעיקר כטלאי (patch) בארונות חיווט לחיבור רכזות.
- **Type 7**. לא מוגדר.
- **Type 8**. כבל STP לשימוש מתחת לשטיחים. למעשה, זהו כבל Type 6 עם מעטפת שטוחה.
- **Type 9**. גירסה plenum-rated של כבל Type 6.

רוב רשתות Token Ring משתמשות בכבל Type 1 או Type 3. אולם IEEE פיתח תקן הנקרא UTP/TR אשר מגדיר את השימוש בכבל UTP קטגוריה 5 בסביבת Token Ring. התקנות Token Ring חדשות רבות ישתמשו כיום בכבל UTP רגיל במקום בכבלי STP היקרים יותר של יבמ. אולם בסביבות בהן יש הפרעות אלקטרומגנטיות תיתכן העדפה של כבל Type 1 STP, מכיון שהסיכוך מקטין את הרגישות להפרעות.



רעיון מפתח

כיום, רוב רשתות Token Ring משתמשות בכבל UTP Type 3 או בכבל STP Type 1 של יבמ. רשתות חדשות יותר עשויות להשתמש ב-UTP רגיל קטגוריה 5.

כאשר כבלי UTP משמשים לחיבור מחשבים לרכזות, הם משתמשים בחיבור RJ-45 התקני. אולם לכבלי STP Type 1 יש מחבר עם 9 פינים בקצה אחד עבור כרטיס ממשק הרשת ומחבר נתונים מיוחד של יבמ (IBM data connector), או Type A connector בקצה השני עבור ה-MAU.

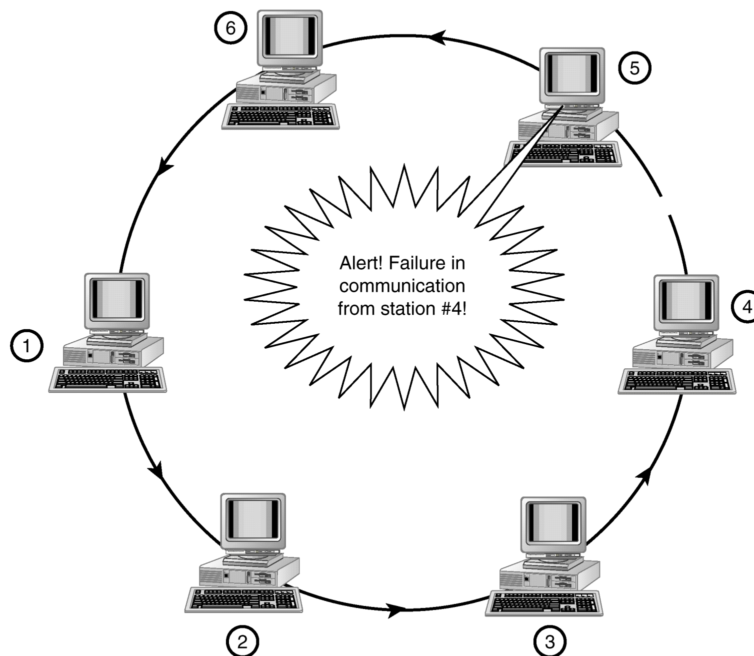
איתות (Beaconing)

תכונה חשובה של רשתות Token Ring היא היכולת שלהן לבצע תיקון-עצמי של בעיות ברשת באמצעות תהליך הנקרא **איתות** (beaconing). ברשת Token Ring, המחשב הראשון שמופעל הופך להיות Active Monitor (תורן פעיל) האחראי לאבטחת תנועת הנתונים סביב הטבעת. כל המחשבים האחרים הופכים ל- Standby Monitors (תורן בהמתנה) בעת הפעלתם.

התפקיד של Active Monitor פשוט. כל שבע שניות הוא שולח מסגרת (frame) מיוחדת לשכן הפעיל הבא הקרוב ביותר (NADN). מנה זו מכריזה על הכתובת של ה- Active Monitor ועל כך שהוא השכן הקודם (NAUN). התחנה המקבלת בודקת את מנת הנתונים ומעבירה אותה הלאה לתחנה הבאה, לאחר שהיא משנה את הכתובת הקודמת. לתחנה השלישית יש כעת מנת נתונים שבה מופיעה הכתובת של ה- Active Monitor והכתובת של השכן הקרוב הקודם. היא מכינה מנת נתונים שתועבר לשכן הבא. באופן זה המנה עוברת בכל הטבעת וחוזרת ל- Active Monitor. עם השלמת הטבעת, יודע ה- Active Monitor שטבעת הרשת שלמה, וכל התחנות ברשת יודעות את הכתובת של השכן הקודם להן ברשת (NAUN).

כפי שניתן לראות בתרשים 7.11, אם מחשב לא שמע מהשכן הקודם לו ברשת לאחר שבע שניות, הוא שולח לטבעת חבילה הכוללת שלושה נתונים: כתובתו, כתובת השכן שלו שלא יצר את הקשר הדרוש, ואת סוג ה**איתות** (beacon). מנה זו עוברת ברשת, ומכריחה את כל המחשבים לבדוק את התצורה שלהם. אם אין תשובה מהשכן הבא, הטבעת יכולה להגדיר את עצמה מחדש ולעקוף את האזור הבעייתי. באופן זה ניתן ליצור רמה מסוימת של סיבולת לתקלות (fault tolerance) ובכך להבטיח רמה גבוהה של יציבות רשת. לדוגמה, היכולת להמשיך לתפקד למרות בעיה באחד המחשבים.

טבלה 7.7 מסכמת מידע אודות ארכיטקטורת רשת Token Ring.



***תרשים 7.11: איתות** (beaconing) הוא התהליך שבו מחשבים ברשת Token Ring מזהים בעיה ומנסים לתקן אותה*

***טבלה 7.7:** סיכום מידע Token Ring*

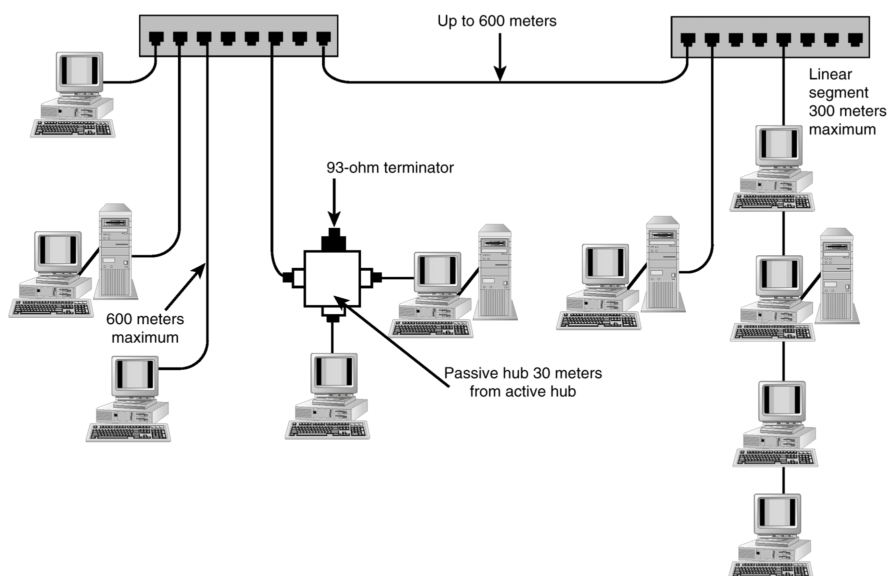
סוג מידע	**מידע Token Ring**
יתרונות:	מהירה ואמינה
חסרונות:	יקרה יותר מפתרונות Ethernet דומים, עלולה להיות קשה לאיתור תקלות
טופולוגיה:	טבעת מחווטת במבנה כוכב (star-ring)
סוג כבל:	סוגי כבלים של יבמ, בדרך כלל Type 1 (STP) ו- Type 3 (UTP) או קטגוריה 5 UTP
סוג מחבר:	IBM Type A או RJ-45
שיטת גישה לתווך רשת:	העברת אסימון (token passing)
אורך מירבי למקטע:	45 מטר (150 רגל) עם UTP, 101 מטר (330 רגל) עם STP
אורך מירבי כולל לרשת:	N/A
מרחק מינימלי בין צמתים (nodes):	2.5 מטר (8 רגל)

טבלה 7.7: *סיכום מידע Token Ring (המשך)*

סוג מידע	מידע Token Ring
מספר מירבי של מקטעים מחוברים:	33 רכזות
מספר מירבי של צמתים במקטע:	תלוי ברכזת
מספר מירבי של צמתים ברשת:	72 צמתים עם UTP, 260 צמתים עם STP
מהירות שידור:	4Mbps או 16Mbps
מפרט IEEE:	802.5

ARCnet (מפרט ANSI 878.1)

ארכיטקטורת ARCnet (Attached Resource Computer Network) היא ארכיטקטורת הרשת הישנה ביותר הנדונה בספר זה. ARCnet פותחה בשנת 1977 על ידי Datapoint Corporation ומספקת מהירות העברה ברשת עד 2.5Mbps בשיטת גישה של העברת אסימון. כמו Token Ring, גם ARCnet מממשת טופולוגיית **טבעת לוגית** (logical ring), אולם כפי שניתן לראות בתרשים 7.12, המבנה הפיסי של הרשת יכול להיות אפיק, כוכב או תערובת של שניהם. בנוסף, רשת אחת יכולה לכלול סוגים רבים של תווך רשת, כמו למשל UTP, כבל קואקסיאלי וכבל סיב-אופטי.



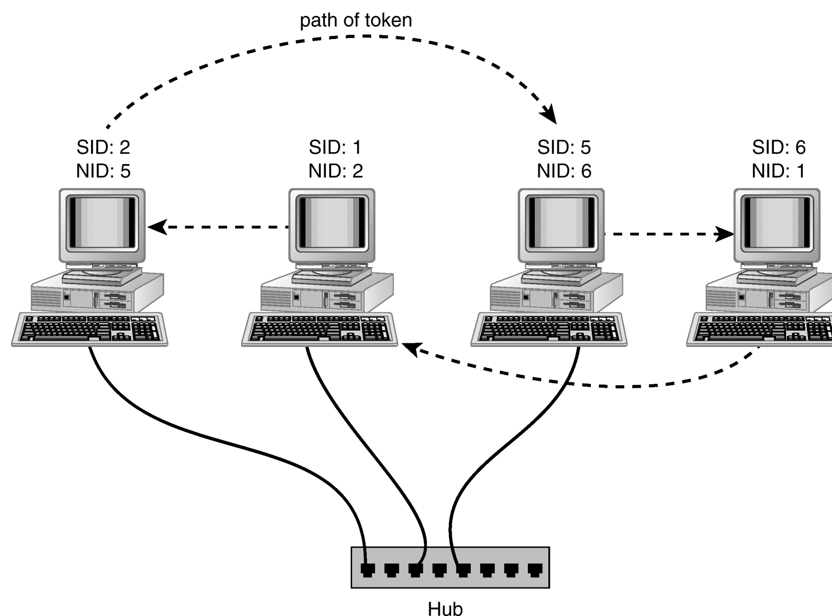
תרשים 7.12: *ARCnet יכולה להשתמש בטופולוגיות כוכב ואפיק באותה רשת*

העברת נתונים ב-ARCnet דומה ל-Ethernet בכך שאותות משודרים בכל הרשת. כל מחשב ברשת מקשיב לאותות המיועדים לכתובת שלו, ומעבד אותות אלה תוך התעלמות מאותות אחרים. רכזות בסביבת ARCnet מחווטות באופן דומה לרשתות כוכב של Ethernet, **ולא** כטבעות לוגיות באופן שרשת Token Ring מחווטת.

מנגנון העברת האסימון של ARCnet שונה מזה של רשתות Token Ring. ב- Token Ring, האסימון עובר מתחנה לתחנה לפי קירבה. לדוגמה, כאשר האסימון נכנס לרכזת ממחשב אחד, הוא עובר דרך הרכזת אל הכניסה המחוברת הבאה, ומשם אל המחשב המחובר. כאשר מחשב זה מסיים עם האסימון הוא חוזר לרכזת, והלאה אל המחשב הקרוב ביותר הבא.

לעומת זאת, ב-ARCnet האסימון עובר ממחשב למחשב על סמך **קוד זיהוי התחנה (SID** - station identifier). כרטיסי ממשק רשת של ARCnet אינם משתמשים בכתובת צרובה כמו Ethernet ו- Token Ring. במקום זאת, על כל כרטיס ממשק רשת יש מפסק DIP המשמש לקביעת SID של המחשב. כתובת זו יכולה להיות בין 1 ל-255 ונקבעת בעת התקנת כרטיס רשת ARCnet במחשב. למעשה, האסימון עובר ממחשב בעל SID של 1 למחשב בעל SID של 2, מ- 2 ל- 3, מ- 3 ל- 4, וכך הלאה לפי הסדר המספרי עד שמחשב בעל SID של 255 מחזיר אותו למחשב בעל SID של 1 (לא משנה הסדר הפיסי של המחשבים ברשת).

מכיון שמרבית רשתות ARCnet אינן מכילות 255 צמתים, המחשבים ברשת לומדים את קוד זיהוי התחנה הבא - **NID** (next station identifier) כדי להימנע מהעברת האסימון לצמתים שאינם קיימים. כאשר מתווסף מחשב לרשת או מוסר מהרשת, או בעת הפעלה ראשונית של הרשת, התחנה בעלת SID הנמוך ביותר (בדרך כלל 1) מזהה את עצמה כתחנה בעלת האסימון ושולחת ברשת שאילתה אל תחנה בעלת SID הגדול באחד מהמספר שלה. אם לא מתקבלת תשובה, היא ממשיכה להגדיל את המספר עד שמתקבלת תשובה. היא לומדת את NID של המחשב שהגיב, ומעבירה למחשב זה את האסימון. האחרון מתחיל בתהליך שאילתה משלו למציאת התחנה הבאה. בסופו של דבר, מחשב כלשהו מגיע אל מחשב 255 בשאילתה שלו, ומשם הוא ממשיך לשאול ל-SID 1. בסיום תהליך זה, המערכת מוגדרת מחדש וכל תחנה יודעת את הכתובת של התחנה הבאה, כפי שמוצג בתרשים 7.13.



תרשים 7.13: האסימון ברשת ARCnet מועבר ממחשב אחד לשני בסדר מספרי

למרות שנוהל זה להעברת אסימון קל להבנה ופועל יפה, הוא סובל ממספר מגבלות. ראשית, יש לשים לב לסדר שבו מוקצות כתובות. האסימון עובר מתחנה אחת לתחנה בעלת הכתובת המספרית הבאה בין אם התחנות קרובות או רחוקות פיסית זו מזו. אם תקצה כתובות המבוססות על קירבה, זרימת התעבורה ברשת תהיה יעילה ומהירה יותר. בנוסף, האסימון עובר במהירות קבועה המגבילה את המהירות הכוללת ברשת.

חיסרון נוסף של ARCnet הוא תהליך התצורה הידני. לכל מחשב חייבת להיות כתובת ייחודית שנקבעת ידנית. מנהל הרשת חייב לעקוב אחר כתובות אלו ולהבטיח שמחשבים חדשים ברשת יקבלו מספרים חדשים. בנוסף, מתג DIP בעל שמונה הסיביות המשמש בכרטיסי ממשק רשת של ARCnet מגביל את מספר התחנות ברשת ל-255.

למרות זאת, קיימות סיבות ברורות לשימוש ב-ARCnet. ארכיטקטורה זו היא אחת הפשוטות והזולות ביותר להתקנה. שיטת העברת האסימון מבטיחה גישה לתווך הרשת ומספקת העברה אמינה של נתונים. ARCnet גם יכולה להעביר נתונים על פני מרחקים ארוכים יותר מאשר ארכיטקטורות אחרות, ויכולה להשתמש בתערובת של סוגי תווך פיסי.

אולם המהירות האיטית של ARCnet, 2.5Mbps, וחוסר היכולת שלה לקישוריות הדדית עם ארכיטקטורות רשת אחרות, מגבילות את המשיכה אליה. למרות שספקים אחדים מפיצים ARCnet Plus עם מהירויות תמסורת המתקרבות ל-20Mbps, השימוש ברשתות ARCnet דועך.

כבלי ARCnet

כפי שהוזכר בסעיף הקודם, רשתות ARCnet יכולות להשתמש בסוגים רבים של כבלים. הסוג הנפוץ ביותר בשימוש הוא כבל קואקסיאלי RG-62A/U 93 אוהם עם מחבר BNC בכל קצה. בטופולוגיית אפיק **מחברי T** (T-connector) מסוג BNC משמשים כמו ברשתות Ethernet 10Base2. בטופולוגיית כוכב, מחברי BNC מחוברים ישירות לרכזת, או לכרטיס ממשק הרשת ללא מחבר T.

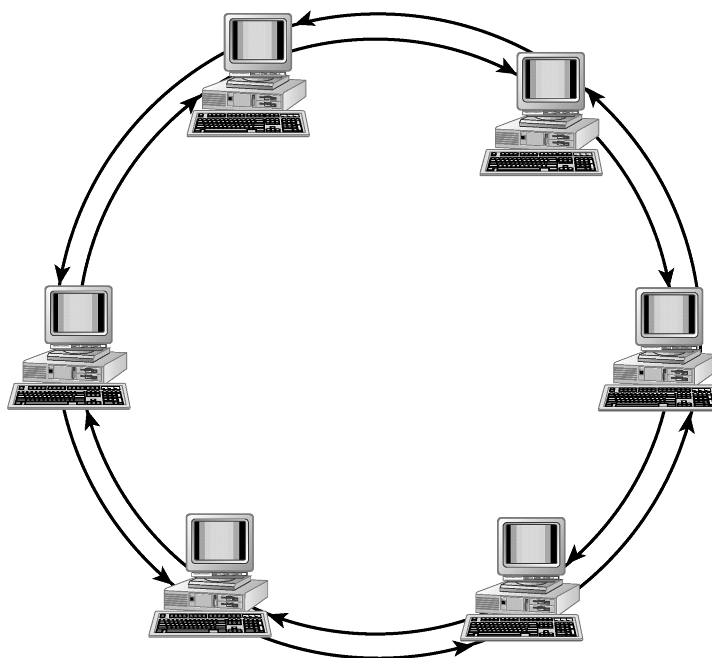
טבלה 7.8 מסכמת מידע אודות ארכיטקטורת רשת ARCnet.

טבלה 7.8: *סיכום מידע ARCnet*

סוג מידע	**מידע ARCnet**
יתרונות:	זולה, קלה להתקנה, אמינה
חסרונות:	איטית, אינה מתחברת טוב למערכות אחרות
טופולוגיה:	כוכב ואפיק
סוג כבל:	כבל קואקסיאלי RG-62A/U (93 אוהם), UTP, סיב-אופטי
סוג מחבר:	BNC, RJ-45, אחרים
שיטת גישה לתווך רשת:	העברת אסימון (token passing)
אורך מירבי למקטע:	600 מטר (2,000 רגל) עם RG-62A/U 121 מטר (400 רגל) עם UTP 3485 מטר (11,500 רגל) עם סיבים אופטיים 30 מטר (100 רגל) מרַכֶּזת פסיבית
אורך מירבי כולל לרשת:	6060 מטר (20,000 רגל)
מרחק מינימלי בין צמתים (nodes):	משתנה
מספר מירבי של מקטעים מחוברים:	משתנה
מספר מירבי של צמתים במקטע:	משתנה
מספר מירבי של צמתים ברשת:	255
מהירות שידור:	2.5Mbps
מפרט IEEE:	אין מפרט IEEE, אך יש ANSI 878.1

FDDI (מפרט ANSI X3T9.5)

רשת FDDI, או ממשק הנתונים המבוזרים בסיב אופטי - Fiber Distributed Data) FDDI (Interface משתמש בכבל סיב-אופטי ובהעברת אסימון ליצירת רשת מהירה ואמינה מאוד הפועלת במהירויות של 100Mbps. היא יכולה לכלול עד 500 צמתים על פני מרחק של 100 ק״מ (60 מייל). FDDI משתמשת בטופולוגיית טבעת עם שתי טבעות הפועלות בכיוונים הפוכים, כפי שמוצג בתרשים 7.14. בעוד שרשתות Token Ring מהוות טבעת לוגית, אך מחווטות פיסית בטופולוגיית כוכב, רשתות FDDI ממומשות כטבעת פיסית אמיתית. אין רכזות, אולם התקנים הנקראים **רכזים** (concentrators) מספקים פעולה דומה.

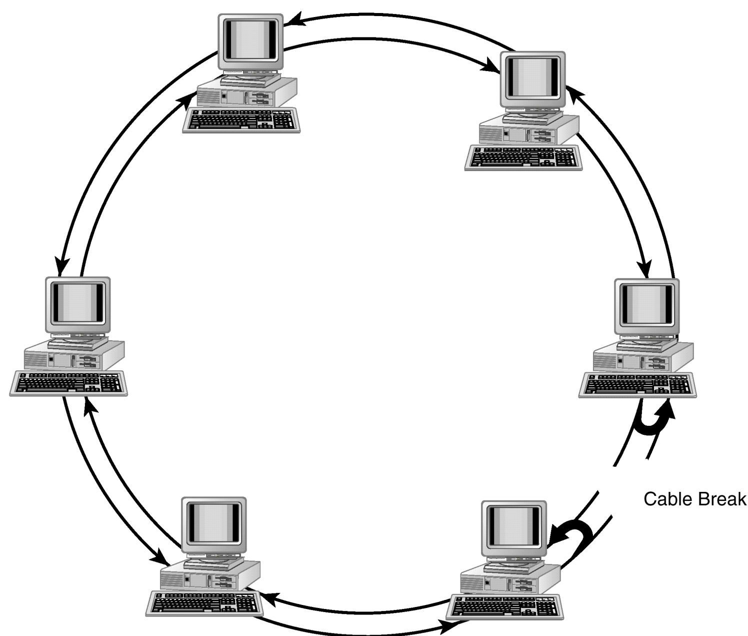


תרשים 7.14: *רשתות FDDI משתמשות בשתי טבעות בכיוונים מנוגדים לאספקת חיבורים אמינים ב-100Mbps*

העברת אסימון ברשת FDDI פועלת באופן שונה מאשר ברשתות Token Ring. בדומה לרשתות Token Ring, מסגרת אסימון עוברת בטבעת, אולם לאחר שידור מסגרת נתונים אחת, מי שמחזיק באסימון FDDI יכול לשדר מסגרות נתונים נוספות לפני שהוא ממתין למסגרת הנתונים הראשונה שתסיים את המעבר סביב הרשת. בנוסף, כאשר מחזיק האסימון סיים לשדר את כל המסגרות שלו, הוא יכול מיידית להעביר את האסימון לתחנה הבאה ותחנה זו יכולה להתחיל לשדר מסגרות. בדרך זו מסגרות רבות עשויות להימצא ברשת בו-זמנית.

FDDI גם תומכת ביכולת לקבוע סדרי עדיפויות של מסגרת נתונים ואסימון. לדוגמה, ניתן לספק לשרתים יכולת לשלוח לרשת יותר מסגרות נתונים מאשר יכולות תחנות אחרות. באופן דומה, שידורי וידאו או נתונים רגישים לזמן יכולים לקבל עדיפות גבוהה יותר כדי שהמנות יסופקו בזמן.

ברשת Token Ring, כל המחשבים מתקשרים דרך רכזות. אם יש נתק בכבל, התחנות האחרות יכולות לזהות זאת בעזרת תהליך **האיתות** (beaconing) ולנתב את המנות סביב התחנה הבעייתית (או הכניסה הבעייתית ברכזת). עם FDDI, כל הנתונים משודרים ב**טבעת הראשית** (primary ring), וה**טבעת המשנית** (secondary ring) מספקת שיטה לפיצוי על נתקים בכבל. כאשר מחשב מזהה שהוא אינו יכול לשדר נתונים לשכנו בתור, הוא מעביר את הנתונים לטבעת המשנית ושולח את הנתונים חזרה ברשת בכיוון ההפוך. כשהמנה מגיעה לקצה השני של הטבעת, במקום שבו הנתק, היא מועברת חזרה לטבעת הראשית וממשיכה בדרכה. כפי שמוצג בתרשים 7.15, מנגנון זה מאפשר לנתונים לעבור ברשת באופן אמין.

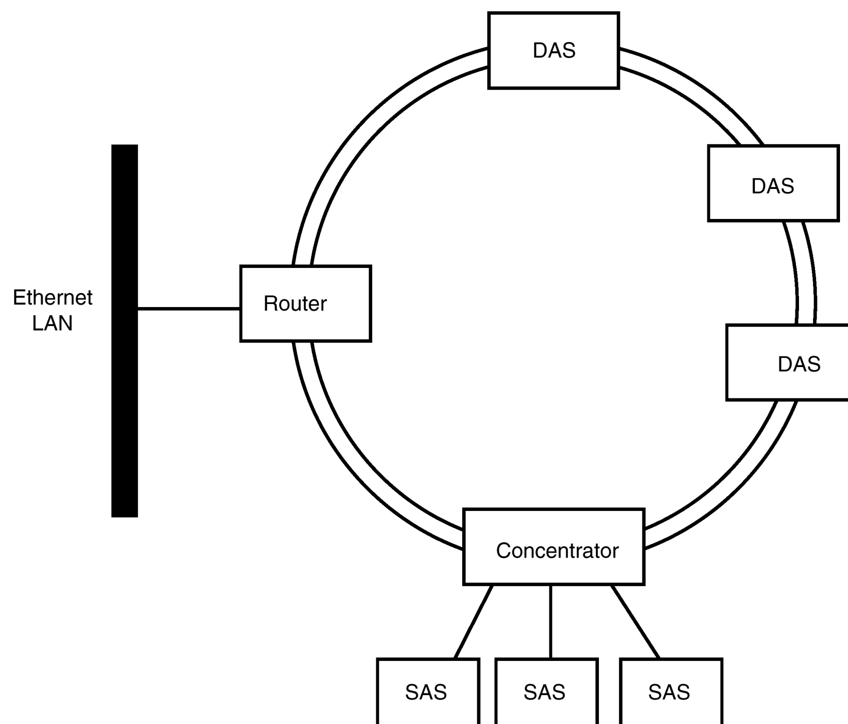


תרשים 7.15: נתק ברשת FDDI גורם למנות להישלח בחזרה בטבעת השנייה

קיימים שני סוגים של כרטיסי ממשק רשת FDDI הנקראים **תחנות בעלות חיבור כפול - DAS** (Dual Attachment Stations) **ותחנות בעלות חיבור יחיד - SAS** (Single Attachment Stations). DAS מחוברות לשתי הטבעות ומיועדות בעיקר עבור שרתים, רכזים, והתקנים אחרים הזקוקים לאמינות המסופקת על ידי המבנה של שתי טבעות. SAS מיועדות לקישור תחנות עבודה אל הרכז. הם מממשות רק קישור טבעת אחד, אולם מכיון שהרכז שאליו הן מחוברות מחובר בדרך כלל לשתי הטבעות, האמינות של הרשת מובטחת.

רכזים דומים לרכזות המשמשות בארכיטקטורות אחרות. **רכזים עם חיבור כפול** (dual attachment concentrators) מחוברים לשתי הטבעות ויש להם כניסות המאפשרות חיבור של תחנות עבודה. **רכזים עם חיבור בודד** (single attachment concentrators) יכולים להיות מחוברים לרכזים עם חיבור כפול, כדי לאפשר חיבור תחנות עבודה נוספות לרשת.

תרשים 7.16 מתאר מימוש רשת FDDI אופיינית. כפי שמוצג בתרשים, נפוץ למצוא התקן כגון **נתב** (router) או **מתג** (switch) המקשר את רשת FDDI לרשת מקומית (LAN). למעשה, השימוש הנפוץ ב-FDDI הוא כרשת **אפיק שידרה** (backbone) המחברת מספר רשתות מקומיות. טכנולוגיית הסיבים האופטיים המשמשת עבור FDDI יקרה מדי לשימוש ברוב הרשתות המקומיות. עם זאת, המהירות, האמינות והיכולת לעבור מרחקים ארוכים הופכות רשת זו לבחירה מצוינת עבור רשת אפיק שידרה.



תרשים 7.16: *רשת FDDI אופיינית יכולה לכלול שרתים, רכזים וקשרים לרשתות אחרות*



טיפ: מכיון ש-FDDI משתמשת בכבל סיב-אופטי, היא גם אפשרית בסביבות הסובלות מהפרעות אלקטרומגנטיות. רשתות הדורשות אבטחה גבוהה עשויות גם הן להשתמש ב-FDDI הודות לחוסר היכולת של גורמים חיצוניים לצותת לשידורים בסיבים אופטיים.

טבלה 7.9 מסכמת מידע אודות ארכיטקטורת רשת FDDI.

טבלה 7.9: סיכום מידע FDDI

סוג מידע	מידע FDDI
יתרונות:	מהירה מאוד, מרחקים ארוכים, בטוחה מאוד, חסינה בפני EMI. אפשרות נתינת עדיפות זמן שידור (למחשב המוגדר "שרת")
חסרונות:	יקרה מאוד, קשה להתקנה
טופולוגיה:	טבעת
סוג כבל:	סיב-אופטי
סוג מחבר:	מיוחד
שיטת גישה לתווך רשת:	העברת אסימון
אורך מירבי למקטע:	N/A
אורך מירבי כולל לרשת:	100 ק"מ (60 מייל)
מרחק מינימלי בין צמתים (nodes):	N/A
מספר מירבי של מקטעים מחוברים:	N/A
מספר מירבי של צמתים במקטע:	N/A
מספר מירבי של צמתים ברשת:	500
מהירות שידור:	100Mbps
מפרט IEEE:	אין מפרט IEEE, מלבד ANSI X3T9.5

סיכום

ארכיטקטורת הרשת הנפוצה ביותר בשימוש כיום היא תקן IEEE 802.3 של Ethernet, הפועלת במהירות 10Mbps באחת מארבע ארכיטקטורות: 10BaseT, 10Base2, 10Base5 ו-10BaseF. 10BaseT מממשת טופולוגיית כוכב באמצעות כבל UTP (זוג שזור לא-מסוכך). 10Base2 ו-10Base5 מממשות טופולוגיית אפיק באמצעות כבל קואקסיאלי Thinnet ו-Thicknet. 10BaseF הוא תקן סיב-אופטי המשמש בדרך כלל כאפיק שידרה לחיבור בין רשתות Ethernet מקומיות אחרות.

כל רשתות Ethernet במהירות 10Mbps משתמשות ב-CSMA/CD (carrier-sense multiple access with collision detection) לבקרת גישה לתווך הרשת. כולן גם משתמשות באחד מארבעה סוגי מסגרת Ethernet: Ethernet 802.3, Ethernet 802.2, Ethernet SNAP ו- Ethernet II. כדי ששני התקנים יוכלו לתקשר ברשת Ethernet, שניהם **חייבים** להשתמש באותו סוג מסגרת (Frame Type).

רשתות Ethernet במהירות 100Mbps זמינות כיום בשתי תצורות: 100BaseT ו-100VG-AnyLAN. 100BaseT מתבססת על רשתות Ethernet קיימות ודורשת UTP Category 5. היא משתמשת ב-CSMA/CD לבקרת גישה לתווך וזקוקה לכרטיסי ממשק רשת (NIC) מיוחדים ורכזות מיוחדות. 100VG-AnyLAN מתוכננת לעבוד על כבלי UTP החל מקטגוריה 3 המשמשים להעברת קול (voice-grade, category 3) ומעלה שיש בהם ארבעה זוגות שזורים של חוט. גם היא דורשת ממשתמשים לשדרג את כרטיסי ממשק הרשת ואת הרכזות שלהם. 100VG-AnyLAN מגיעה למהירויות של 100Mbps על ידי שימוש בשיטת גישה חדשה הנקראת **עדיפות דרישה** (demand priority) שבה רכזות חכמות שולטות על איזה מחשב יכול לשדר בכל רגע.

רשתות Ethernet הגיעו לרמת פופולריות כה גבוהה בעיקר מכיון שאינן יקרות, הן קלות למימוש ומהירות מספיק עבור רוב הרשתות המודרניות. החיסרון העיקרי שלהן הוא במצבים של תעבורת רשת כבדה, שבהם שיטת הגישה המבוססת **התמודדות** (contention) הופכת לבלתי יעילה.

מעבר ל-Ethernet, ארכיטקטורת רשת נפוצה נוספת היא Token Ring של יבמ. רשתות Token Ring מעבירות כל העת אסימון כדי לקבוע איזה מחשב יכול לשדר מידע. מחשב אינו יכול לשדר מסגרות נתונים אל הרשת, אלא אם האסימון נמצא אצלו.

רשתות Token Ring ממומשות כ**טבעת לוגית** (logical ring), אולם מחווטות פיסית בטופולוגיית כוכב. כדי להשיג זאת, רכזות Token Ring הנקראות MAU (Multistation Access Units), מחווטות פנימית כטבעת, וניתן לחבר יחד מספר רכזות ליצירת טבעת גדולה יותר.

רשתות Token Ring משתמשות בעיקר בכבלי Type 1 (STP) ו- Type 3 (UTP) כפי שמוגדרים על ידי מערכת הכבלים של יבמ. תכונה נוספת של רשתות Token Ring היא היכולת לתיקון עצמי של הרשת באמצעות תהליך הנקרא **איתות** (beaconing) שבו תחנות מודיעות לתחנות אחרות ברשת כשהן לא מקבלות שידורים מתחנות מסוימות.

רשתות Token Ring נפוצות במצבים של תעבורת רשת כבדה, או כאשר האמינות חשובה מאוד.

ARCnet היא ארכיטקטורת רשת ותיקה יותר המשתמשת במערכת העברת אסימון עם כתובות מספריות שתצורתן מבוצעת ידנית על כרטיסי ממשק הרשת. הטופולוגיה יכולה להיות כוכב, אפיק או תערובת של השתיים, ותווך הרשת יכול להיות קואקסיאלי, UTP, סיב-אופטי, או תערובת של כולם. ARCnet היא ארכיטקטורה קלה וגמישה מאוד, אולם היא מוגבלת על ידי מהירות שידור נתונים של 2.5Mbps ועל ידי ההגבלה ל-255 צמתים. למרות שגרסאות מהירות יותר של ARCnet יוצאות לשוק, ארכיטקטורת רשת זו נעלמת מהנוף.

לבסוף, FDDI (Fiber Distributed Data Interface) היא ארכיטקטורת רשת חדשה יותר המבוססת על כבלי סיב-אופטי שיכולה לספק מהירויות שידור נתונים עד 100Mbps על פני מרחקים של 100 ק״מ (60 מייל). היא משתמשת בהעברת אסימון. אולם, שלא כמו Token Ring, מחשב עם האסימון יכול לשדר מספר מסגרות לרשת עוד לפני שהמסגרת הראשונה סיימה את המסע שלה סביב הטבעת. בנוסף, שלא כמו ב- Token Ring, FDDI אינה משתמשת ברכזות אלא מממשת טופולוגיית טבעת אמיתית.

FDDI משתמשת בשתי טבעות בכיוונים מנוגדים. נתונים משודרים בטבעת הראשית, והטבעת השנייה משמשת למטרות גיבוי. אם מחשב מזהה נתק בקו, הנתונים מוחזרים בטבעת השנייה בכיוון ההפוך. באופן זה ניתן לשמור על חיבור אמין בין אתרים שנמצאים על הטבעת.

בגלל העלות הגבוהה של כבלי סיב-אופטי והתקנים נלווים, FDDI משמשת בעיקר כאפיק שידרה המחבר בין רשתות אחרות.

8

פרוטוקולי רשת

לאחר הקמת החיבור הפיסי בין שני מחשבים וקביעת אופן העברת הנתונים על פני תווך הרשת (network media), תצטרך להשתמש בפרוטוקולי הרשת כדי ליצור את התקשורת ברשת. לאחר קריאת פרק זה תוכל:

- ✯ להסביר את תפקיד הפרוטוקולים ברשת.
- ✯ לתאר את ההבדל בין פרוטוקולים **חסרי-קישור** (connectionless) **ו**מוכווני-קישור (connection-oriented).
- ✯ לזהות את סוגי הפרוטוקולים השונים המשמשים ברשתות מחשבים.
- ✯ לדעת כיצד להתקין פרוטוקולי רשת.
- ✯ להבין את תפקיד **NDIS** ו-**ODI** בתקשורת רשתות.
- ✯ להסביר כיצד פרוטוקולים משמשים ברשתות מיקרוסופט ל**פענוח שמות** (name resolution).

תפקיד הפרוטוקולים

כאשר שני מנהיגים חשובים נפגשים פנים אל פנים, הם מודאגים מאוד מהפרוטוקולים המשמשים לתקשורת האישית ביניהם. האם עליהם ללחוץ ידיים? האם עליהם לחבק זה את זה, או לנשק בלחי פעם אחת או פעמיים? עד כמה הם אמורים להתקרב זה לזה? כיצד עליהם לשבת ליד השולחן ובאיזה סדר? באיזו שפה עליהם לדבר? כל הגורמים האלה יכולים להשפיע מאוד על הצלחה או כישלון של פגישת צמרת בינלאומית או פוליטית. אם ייעשה שימוש בפרוטוקולים הלא נכונים, לא תתקיים התקשורת הראויה.

כך גם ברשתות המחשבים, פרוטוקולי התקשורת חיוניים לזרימת התעבורה ברשת. כדי ששני מחשבים יוכלו לתקשר זה עם זה , עליהם להשתמש באותם פרוטוקולים.

כפי שאתה כבר יודע, הפעילות ברשת רבה. מכיון שפרוטוקולים פותחו כדי לענות על כל סוגי הפעולות ברשת, הם בדרך כלל מקובצים יחד ל**מחסניות פרוטוקול** (protocol stacks) או **מערכות פרוטוקול** (protocol suites). שתי מערכות הפרוטוקול הנפוצות ביותר הן TCP/IP, המשמשת באינטרנט וברשתות גדולות רבות, ו-IPX/SPX המשמשת ברשתות Novell NetWare.

בעוד שבהמשך הפרק נדון בפירוט במערכות הפרוטוקול השונות, חשוב להבחין כבר כעת בין סוגי פרוטוקולים שייכללו במערכות הפרוטוקול. אנו מזהים שתי הבחנות עיקריות בין פרוטוקולים:

- פרוטוקולים חסרי-קישור לעומת פרוטוקולים מוכווני-קישור,
- פרוטוקולים מנותבים לעומת פרוטוקולים חסרי-ניתוב.

בכל אחת מהגדרות אלו נדון בסעיפים הבאים.

פרוטוקולים חסרי-קישור לעומת מוכווני-קישור
Connectionless versus Connection-Oriented Protocols

כאשר אתה שולח למישהו מכתב בדואר, אתה שם אותו בתיבת דואר, וזהו. אינך יודע מתי או אם בכלל המכתב יגיע, וגם אינך מקבל אישור כלשהו כשהמכתב מתקבל ביעדו. אין לך כל הבטחה שהמכתב יגיע.

מצד שני, כאשר אתה מתקשר למישהו בטלפון, יש השהייה קצרה בזמן הקמת ההתקשרות בינך ובין זה שאליו אתה מתקשר. לאחר שדיברתם זמן מה, אתה מניח את השפופרת וההתקשרות מסתיימת. בתקשורת מסוג זה מובטח לך שהתקיים קשר והנמען קיבל את המסר.

ברשת מחשבים, תקשורת **חסרת-קישור** (connectionless) דומה מאוד למשלוח מכתב בדואר. פרוטוקולים המשתמשים בתקשורת חסרת-קישור אינם דורשים חיבור ראשוני כלשהו (או הבטחת חיבור כזה), ומניחים שהנתונים יעברו ליעדם. שירותים חסרי-קישור מהירים מאוד, מכיון שאינם מחייבים תקורה כלשהי ואינם מספקים **רצף סדרתי** (sequencing) של מנות נתונים. הנתונים רק משודרים, ומיון סדר המנות הוא משימה שנעשית על ידי פרוטוקולים ברמות גבוהות יותר. מנות נתונים בתקשורת חסרת קישור נקראות במקרים רבים **צרור נתונים** (datagrams). לדוגמה, תחנת רדיו המשדרת באינטרנט.



רעיון מפתח

תקשורת חסרת-קישור (connectionless) כוללת העברת נתונים פשוטה, ללא הבטחה שהם יתקבלו ביעד.

לעומת זאת, תקשורת **מוכוונת-קישור** (connection-oriented) דומה לשיחת טלפון, שבה מוקם קשר בין שני מחשבים **לפני** שהתקשורת יכולה להתחיל. לאחר יצירת הקשר, הנתונים משודרים ברצף סדרתי. כאשר כל מנה (או קבוצת מנות, במקרים מסוימים) מגיעה למקבל, נשלח אישור מסירה בחזרה לשולח. אם יש שגיאות כלשהן, הנתונים מועברים שוב. כאשר כל הנתונים הועברו, הקשר מסתיים. תקשורת מוכוונת-קישור נקראת לעיתים תקשורת **אמינה** (reliable), כי מובטחת בה העברת הנתונים מהמקור אל היעד. לדוגמה, משלוח דואר אלקטרוני. אם המסר לא הגיע ליעדו מתקבלת הודעת שגיאה.

בפרוטוקולי תקשורת מוכוונת-קישור משתמשים כאשר רוצים להבטיח העברה אמינה של נתונים. הם משמשים במיוחד בחיבורי WAN, בהם התווך הפיסי אינו אמין ועלול לגרום לשגיאות בהעברה הנתונים. פרוטוקול TCP הוא דוגמה לתקשורת מוכוונת-קישור.



רעיון מפתח

תקשורת מוכוונת-קישור (connection-oriented) כרוכה בהקמת קשר אמין בין שני מחשבים **לפני** תחילת שידור הנתונים. נתונים מועברים בצורה סדרתית, שבה קבלה מוצלחת של כל מנה (או קבוצת מנות) מאושרת על ידי המקבל.

פרוטוקולים מנותבים לעומת חסרי-ניתוב
Routers versus Non-Routable Protocol

הבחנה עיקרית נוספת בין מערכות פרוטוקולים היא התאמתן לרשתות בהיקף גדול, או רשתות של תאגידים גדולים. התקנים הנקראים **נתבים** (routers) מאפשרים לחבר מספר רשתות מקומיות כדי ליצור רשת גדולה יותר. פרוטוקולי רשת אחדים, כגון TCP/IP ו-IPX/SPX, יכולים לפעול בשילוב נתבים לבניית רשתות גדולות, לכן הם נקראים פרוטוקולים **מנותבים** (routable). לעומתם, פרוטוקולים **חסרי-ניתוב** (non-routable), כגון NetBEUI, תוכננו לרשתות קטנות ולא ניתן להרחיבם לשימוש עם נתבים לבניית רשתות גדולות. אחד הגורמים שישפיעו על בחירת פרוטוקול עבור הרשת שלך יהיה השיקול של הקמת רשת גדולה יותר בעתיד.

פרוטוקולים

ברשתות מחשבים אישיים אנו מכירים שלושה פרוטוקולים עיקריים:

- ✯ TCP/IP,
- ✯ IPX/SPX (Novell NetWare),
- ✯ NetBEUI.

בשנים האחרונות גדל השימוש ב-TCP/IP באופן משמעותי כתוצאה מהעניין ההולך וגובר **באינטרנט**. עם זאת, נפוצות גם התקנות גדולות המשתמשות הן ב-IPX/SPX והן ב-NetBEUI. שלושה פרוטוקולים אלה יידונו בהמשך הפרק, ולאחר מכן נאזכר בקצרה פרוטוקולי רישות נוספים הזמינים בשוק.

TCP/IP

מערכת פרוטוקולי TCP/IP נקראת במקרים רבים **מערכת פרוטוקול אינטרנט** (Internet protocol suite), מכיון שהיא פותחה במהלך פיתוח האינטרנט. לאחר מכן שולב הפרוטוקול בכל שרתי UNIX ונכנס לשימוש נרחב ברשתות גדולות הנקראות במקרים רבים **רשתות תאגיד** (enterprise networks). יכולת המידרוג של TCP/IP מרשתות קטנות לגדולות, והעניין הרב בחיבור רשתות מקומיות לאינטרנט אפשרו ל-TCP/IP להתפתח לפרוטוקול הרשת הנפוץ ביותר היום.

מכיון שפרוטוקולי TCP/IP פותחו לפני שהוגדר מודל הייחוס OSI, הם אינם תואמים במדויק לשכבות המודל (כבר אמרנו שמודל OSI הוא מודל תיאורטי/התייחסותי). חבילת פרוטוקולי TCP/IP כוללת את הפרוטוקולים הבאים:

- ✯ **IP** (Internet Protocol). כל הכתובות והניתובים ברשת TCP/IP מנוהלים על ידי IP. הפרוטוקול מספק תקשורת מהירה, גם אם לא אמינה, בין צמתים ברשת על ידי שירות חסר-קישור (connectionless datagram service).
- ✯ **VLSM** (Vriable Lenght Subnet Mask) מאפשר חלוקת הרשת לרשתות משנה, שחלק מהן מחולק שוב לרשתות משנה, וכך הלאה.
- ✯ **ARP** (Address Resolution Protocol). ARP הוא פרוטוקול **שכבת רשת התקשורת** (network layer) הממפה כתובות חומרה (MAC Address) לכתובות IP כדי להעביר מנות במקטע הרשת המקומית.
- ✯ **ICMP** (Internet Control Message Protocol). פרוטוקול ICMP פועל בשילוב עם IP לביצוע הליכי בקרת שגיאות. ICMP יכול לזהות תנאי שגיאה ברשת ולהזהיר את IP מהעברת נתונים בקטעי רשת מסוימים.
- ✯ **IP Multicasting** ו- **IGMP**
- ✯ **IPv6 - IPng** גירסה מתקדמת של פרוטוקול IP.
- ✯ **UDP** (User Datagram Protocol). UDP מספק שירות העברה חסרת-קישור (connectionless) מעל פרוטוקול IP.

- ✯ **TCP** (Transmission Control Protocol). TCP הוא הפרוטוקול העיקרי של **שכבת התעבורה** (Transport Layer) במערכת הפרוטוקולים TCP/IP. הוא מספק שירות Connection-Oriented להעברת נתונים אמין, בשילוב עם IP (המוגדר בסעיף הבא). בעת יצירת קשר, הפרוטוקול משתמש בכתובת **כניסה** (Port Access) כדי לקבוע לאיזו כניסה מיועדת המנה. TCP גם מספק את היכולת לפצל הודעות ולהרכיב מחדש מנות באמצעות **רצף סדרתי** (sequencing).
- ✯ **FTP/TFTP** (File Transfer Protocol). FTP מיועד להעברת קבצים בין מחשבים.
- ✯ **BOOTP** איתחול תחנת עבודה, שאין בה דיסק קשיח, מהשרת.
- ✯ **DHCP** (Dynamic Host Configuration Protocol) יכולת הקצאה של כתובת IP באופן דינמי.
- ✯ **Telnet**. בעזרת Telnet, משתמשים יכולים להיכנס למערכות רחוקות דרך האינטרנט ולפעול בהן.
- ✯ **SMTP** (Simple Mail Transport Protocol). SMTP מגדיר את התקן עבור שידור דואר אלקטרוני באינטרנט.
- ✯ **RIP** (Routing Information Protocol). פרוטוקול שבעזרתו הנתבים קובעים את הדרך הקצרה והפנוייה ביותר להעברת המידע ברשת.

מערכת פרוטוקולי TCP/IP היא כעת ברירת המחדל של Windows 2000.

כתובות IP (IP Address)

ברשתות TCP/IP מוקצית לכל מחשב **כתובת IP** בת 32 סיביות, לדוגמה:

192.168.24.123

כתובת זו מחולקת לארבעה בתים בני שמונה סיביות כל אחד (octets), שכל אחד מהם נכתב כמספר עשרוני שערכו בין 0 ל-255, והם מופרדים זה מזה בנקודה ("dot"). חלק מכתובת IP הוא **קוד זיהוי הרשת** (network id) אליה הוא שייך, ושאר חלקי הכתובת מציינים את **קוד זיהוי מארח** (host id) המציין את המחשב של המשתמש. לדוגמה, הצירוף 24.123 בכתובת שהוצגה קודם עשוי לזהות מחשב מסוים בתוך רשת TCP/IP שכתובתה 192.168.



טיפ: חשוב על חלוקה זו של רשת/מארח כמספר טלפון. למספר טלפון יש קידומת אזור חיוג (ו/או מדינה) ומספר מקומי.



הערה: ברישות TCP/IP, המונח מארח (host) מתייחס למחשב ברשת.



רעיון מפתח

כדי לאפשר הספקת נתונים נכונה, כל כתובת IP חייבת להיות ייחודית בכל הרשת. בנוסף, אם אתה מחובר לאינטרנט, כל כתובת IP שבה אתה משתמש חייבת להיות ייחודית בכל רשת האינטרנט.

בעת הפעלת הרשת המקומית שלך באפשרותך לבחור כל תחום כתובות IP שתרצה. אולם, כאשר תחבר את הרשת לאינטרנט, ספק שירותי האינטרנט שלך (ISP) ימסור לך תחום כתובות IP שיהיה תקף עבורך.

כאמור, כל IP Address מחולקת ל-4 יחידות (classes) שהחלוקה הלוגית שלהם היא כתובת לרשת וכתובת לעמדה. קיימים שלושה סוגי Classes והם:

- **Class A**. כתובות אלו מיועדות לרשתות גדולות במיוחד. המשתמשות בבית (octet) הראשון לזיהוי הרשת ובשאר לכתובת העמדות. כתובות Class A בין 1.0.0.0 לבין 127.255.255.255 .
- **Class B**. כתובות אלו מיועדות לרשתות בינוניות. המשתמשות בשני הבתים הראשונים לזיהוי הרשת, ובשני הבתים האחרים לכתובת העמדות. כתובות Class B בין 128.0.0.0 לבין 191.255.255.255 .
- **Class C**. כתובות אלו מיועדות לרשתות קטנות. המשתמשות בשלושת הבתים הראשונים לזיהוי הרשת ובבית אחד לכתובת העמדות. כתובות Class C בין 192.0.0.0 לבין 223.255.255.255 .

קיימים שני Class נוספים:

- **Class D**. בין 224.0.0.0 לבין 239.255.255.255 .
- **Class E**. בין 240.0.0.0 לבין 255.255.255.255 .

חומר נוסף על פרוטוקולים באינטרנט תוכל למצוא בספר **תקשורת מחשבים, פרוטוקולים וארכיטקטורות רשת**, גולן מוגרבי, הוצאת הוד-עמי ובספר **המדריך השלם לטכנאי PC - רשתות תקשורת**, דורון סיון, הוצאת הוד-עמי.

subnet masks

כשאתה מתכונן להתקשר למישהו בטלפון, כיצד אתה יודע אם צריך לחייג תחילה את קידומת אזור החיוג, או שניתן לחייג את המספר המקומי בלבד? בארה"ב התשובה נמצאת בשימוש בקידומת אזור חיוג בת 3 ספרות, ובארץ - שתי ספרות. בהנחה שאתה יודע את אזור החיוג שלך ואתה מקבל מספר טלפון בעל אזור חיוג התואם לשלך, אתה יודע שאין צורך לחייג את הקידומת. אולם כשנמסר לך מספר טלפון בעל קידומת שונה, עליך לחייג תמיד את קידומת אזור החיוג, כדי להגיע למספר הטלפון הזה.

מחשבים ברשתות TCP/IP פועלים בצורה דומה. אולם בעוד שאתה יודע ששלוש הספרות הראשונות של מספר טלפון הן קידומת אזור החיוג, מחשבים אינם יודעים מייד כמה מתוך 32 הסיביות בכתובת IP מייצגות את הרשת (Network ID) וכמה מהן מייצגות את זיהוי המארח (Host ID) ברשת. כדי להבחין בין זיהוי הרשת לבין זיהוי

המארח, משתמשים המחשבים ב-Subnet mask האומרת להם **כיצד** לקרוא את הכתובת.



רעיון מפתח

בעת משלוח מנת נתונים אל מחשב אחר ברשת TCP/IP, המחשב משתמש ב-Subnet Mask כדי לקבוע את חלקי הרשת והמארח בכתובת היעד.

ב-Subnet Mask המספר 255 מציין את כתובת הרשת והמספר 0 מציין את כתובת העמדה. דוגמה ל- Subnet Mask : 255.255.0.0 המתאים לכתובת מ-Class B.

Dynamic Host Configuration Protocol - DHCP

כאשר רשתות גדולות החלו להשתמש ב-TCP/IP, תהליך הקצאה ידנית של כתובות IP לכל מחשב הפך מסורבל. מעקב אחר כתובות IP שכבר הוקצו הסתבך והלך כאשר מחשבים הועברו ממקום למקום בארגון. כדי לפשט את משימת הקצאת כתובות IP, פיתחו מהנדסי אינטרנט את פרוטוקול **DHCP** (Dynamic Host Configuration Protocol) המשמש להקצאת כתובת IP דינמית**.**

כדי להשתמש ב-DHCP, מפעילים שרת DHCP במקום כלשהו ברשת, ומספקים לו תחום כתובות IP שמתוכן היא יכולה להקצות באופן דינמי כתובת לכל מחשב שמבקש. אחר כך צריך לעבור בין כל מחשבי הלקוח ברשת ולהגדיר להם בקשת כתובת IP משרת DHCP. כאשר מחשבים אלה מאותחלים לראשונה (ובכל פעם שיופעלו), הם משדרים הודעה (broadcast message) ברשת המקומית המבקשת כתובת IP משרת DHCP. שרת זה מקצה כתובת לכל מחשב המבקש זאת, עד שאוזלות לו כל כתובות IP.



הערה: למעשה, כל כתובת IP חכורה (leased) למחשב הלקוח לפרק זמן נתון, כל עוד הוא מקיים את הקשר. ניתן לחדש חכירת כתובת בכל עת שהמחשב זקוק לה.

אחד היתרונות של DHCP הוא בכך שניתן להעביר מחשבים בחברה ממקום למקום ללא דאגה לכתובת IP שלהם. כאשר מחשב מחובר למקטע (segment) רשת אחר ומופעל, הוא משדר הודעה במקטע אליו הוא שייך ומקבל כתובת IP משרת DHCP במקטע הרשת החדש שלו. תהליך זה מאפשר למנהלי רשתות להקצות במרוכז תחומי כתובות IP לשרתי DHCP ולעקוב בקלות רבה יותר אחר הכתובות המוקצות.



רעיון מפתח

DHCP מספק מנגנון להקצאה דינמית של כתובות IP.

IPX/SPX

כמו TCP/IP, מערכת פרוטוקול IPX/SPX המשמשת ברשתות Novell NetWare מתאימה לרשתות קטנות וגדולות כאחד. מערכת פרוטוקולי NWLINK היא המימוש של מיקרוסופט לפרוטוקולי IPX/SPX. NWLINK גם מספקת תמיכה לשמות NetBIOS שיידונו בסעיף הבא. בעת יישום פרוטוקולי IPX/SPX ברשתות Ethernet יש לדאוג לכך שכל המחשבים ישתמשו ב**סוג מסגרת** (frame type) זהה. קיימים ארבעה סוגים של מסגרות נתונים ב-Ethernet: Ethernet 802.2, Ethernet 802.3, Ethernet SNAP ו-Ethernet II. אם הרשת עובדת לאט יש להגדיר את סוג המסגרת באופן ידני. במצב זיהוי מסגרת באופן אוטומטי יבחר סוג המסגרת הנמוך ביותר - Ethernet 802.3.

רישות מיקרוסופט (NetBIOS/NetBEUI/SMB)

יבמ ומיקרוסופט פיתחו במשותף את פרוטוקולי NetBIOS (Network Basic Input Output System) ו-NetBEUI (NetBIOS Extended User Interface) כדי לתמוך בתקשורת רשתות קטנות ובינוניות. NetBIOS ו-NetBEUI הם שני פרוטוקולים נפרדים שנוטים לבלבל ביניהם. רכיבי הרישות של מיקרוסופט כוללים:

- **Redirector - תוכנית ניתוב.** גורמת למשאבי רשת להיראות כאילו הם משאבים מקומיים. מעבירה בקשות למשאבי רשת אל שרת הרשת המתאים.
- **Server Message Block (SMB).** מספק תקשורת **שוויונית** (peer-to-peer) בין תוכנת הניתוב שבמחשב לקוח לבין תוכנת השרת בשרת קבצים.
- **NetBIOS.** פותח Session בין מחשבים ושומר על הקשר ביניהם.
- **NetBEUI.** מספק העברת נתונים. פרוטוקול לרשתות קטנות המגדיר את עצמו באופן אוטומטי.

NetBIOS

NetBIOS הוא פרוטוקול **שכבת Session** המאפשר למחשבים לתקשר ברשת מקומית קטנה:

- כל מחשב ברשת NetBIOS משתמש בשם ייחודי בן 15 תווים לזיהוי עצמו (שמות NetBIOS כוללים למעשה 16 תווים, כשהתו הנוסף הוא הקסדצימלי ומיועד לזיהוי השירות שיצר את השם. אולם המשתמש יכול לראות רק את 15 התווים הראשונים של השם).
- כדי להעביר נתונים בין מערכות, מקים NetBIOS **מושב מכוון-קישור** (Connection-Oriented Session) בין מחשבים. NetBIOS אחראי להקמה, תחזוקה וסיום הקשר, בנוסף להבטחה שכל הנתונים מועברים כראוי (checkpoints).
- ניתן לבצע תקשורת **חסרת-קישור** (Connectionless) באמצעות NetBIOS.
- NetBIOS משתמש בשיטת מנות שידור לכל (broadcast) לזיהוי מחשבים אחרים ברשת המקומית. מחשבים משדרים לכל את שמותיהם בפרקי זמן קצובים, כדי שמחשבים אחרים יוכלו למצוא אותם ולגשת למשאבי הרשת.

NetBIOS עצמו הוא פרוטוקול **חסר-ניתוב** (non-routable), שמסתמך על פרוטוקול בסיסי (כגון TCP/IP ,IPX/SPX או NetBEUI) לקיום התעבורה ברשת. למרות שתוכנן בעיקר לפעול "מעל" פרוטוקול NetBEUI, הוא יכול לפעול גם מעל TCP/IP בעזרת מנות NBT (NetBIOS over TCP/IP).

NetBEUI

NetBEUI הוא פרוטוקול פשוט, מהיר ויעיל ששולט בשכבת התעבורה ובשכבת רשת התקשורת. הוא מיועד לשימוש עם NetBIOS ברשתות לקבוצות עבודה קטנות. מכיון ש-NetBEUI משולב בכל מערכות ההפעלה של מיקרוסופט, תמצא שהוא משמש במקרים רבים בסביבות קטנות לאספקת תקשורת רשת מהירה. הוא אינו דורש זיכרון מערכת רב, וזהו יתרון גדול כאשר יש צורך לכלול מחשבי DOS ברשת.

מכיון ש-NetBEUI הוא חסר-ניתוב, קשה להשתמש בו ברשתות גדולות, ולכן מחליפים אותו בדרך כלל ב-TCP/IP או IPX/SPX.



רעיון מפתח

NetBEUI הוא פרוטוקול תעבורה פשוט, מהיר וחסר-ניתוב המשמש ברשתות של קבוצות עבודה קטנות.

SMB

פרוטוקול SMB (Server Message Block) הוא פרוטוקול שכבת תצוגה שמשמש בדרך כלל ברשתות מיקרוסופט לתקשורת בין תוכנת הניתוב לבין תוכנת השרת. לדוגמה, אם ברצונך להשתמש במנהל הקבצים או בסייר חלונות, כדי לראות רשימה של קבצים הנמצאים במחשב Windows NT Server, המחשב שלך יקים תחילה חיבור רשת אל שרת הקבצים בעזרת פרוטוקול כמו NetBEUI או TCP/IP. על פני חיבור זה, ייפתח מושב (session) של NetBIOS בין תוכנת הניתוב של תחנת העבודה שלך ובין תוכנת השרת שבשרת הקבצים. לאחר הקמת מושב זה, שני המחשבים ישדרו מנות SMB הלוך ושוב כדי שתוכל לראות את רשימת הקבצים.

SMB גם מאפשר למחשבי Windows קישוריות הדדית עם שרתי קבצים המריצים את פרוטוקול LAN Manager הישן יותר של מיקרוסופט.



רעיון מפתח

פרוטוקול SMB (Server Message Block) **הוא פרוטוקול שכבת התצוגה המספק תקשורת בין תוכנות ניתוב של** Windows **לבין שרתי קבצים.**

תוכנת ניתוב (Redirector)

תוכנת הניתוב (redirector) היא רכיב תוכנה המאפשרת למשתמשים לגשת למשאבים כאילו היו משאבים מקומיים.

פרוטוקולים אחרים

למרות ש-TCP/IP, IPX/SPX ו-NetBEUI הם הפרוטוקולים העיקריים כיום ברשתות מחשבים אישיים, כדאי שתכיר מספר פרוטוקולים נוספים. המשך סעיף זה מתאר בקצרה מספר פרוטוקולי רישות כאלה.

AppleTalk

פרוטוקול AppleTalk הגדיר את ארכיטקטורת הרשת ברשתות מקינטוש רבות, וכולל מערכת מקיפה של פרוטוקולים.

DECnet

DECnet היא המימוש של חברת **DIgital והיום Compaq**, לארכיטקטורת הרשת הדיגיטלית שלה **- DNA** (Digital Network Architecture).

DLC

DLC - Data Link Control הוא פרוטוקול חסר-ניתוב המתוכנן לתקשורת בשכבת קישור הנתונים עם מחשבים גדולים של יבמ ועם מדפסות רשת של Hewlett-Packard. מכיון שזהו פרוטוקול ברמה נמוכה שאין לו קשר עם תוכנת הניתוב של Windows, או שירותים אחרים בשכבות הגבוהות, הוא אינו נפוץ ברשתות מחשבים אישיים.



הערה: כדי להפעיל מדפסות רשת של HP, צריך להתקין את DLC רק על המחשב המשמש כשרת הדפסה שהמדפסת מחוברת אליו. אין צורך להתקין את DLC במחשבי לקוחות המדפיסים למדפסת זו באמצעות שרת ההדפסה.



טיפ: פרוטוקול DLC הוא חסר-ניתוב ומשמש לתקשורת ברמה נמוכה עם מחשבים גדולים של יבמ (כגון mainframe), ועם מדפסות רשת בלבד.

NFS

NFS - Network File System הוא פרוטוקול המשמש בעיקר במחשבי Unix לאספקת פעולות כמו בתוכנת הניתוב של Windows.

OSI

מערכת פרוטוקולים שפותחה על ידי ארגון התקנים הבינלאומי ISO נפוץ בעיקר במערכות מחשבים גדולות.

SNA

SNA - System Network Architecture של יבמ, בדומה ל-DECnet ו-OSI, הוא למעשה מערכת שלמה של פרוטוקולים הנמצאים בשימוש נרחב במחשבים גדולים ומחשבי AS/400 של יבמ. שניים מהפרוטוקולים ב-SNA הם :

- Advanced Peer-to-Peer Communications (APPC). מספק שירותים בשכבת התעבורה ובשכבת המושב המאפשרים רישות **שוויוני** (peer-to-peer).
- Advanced Peer-to-Peer Networking (APPN). מספק חיבורים בין מחשבים בשכבת רשת התקשורת ובשכבת התעבורה. מיועד לשימוש עם פרוטוקול APPC.



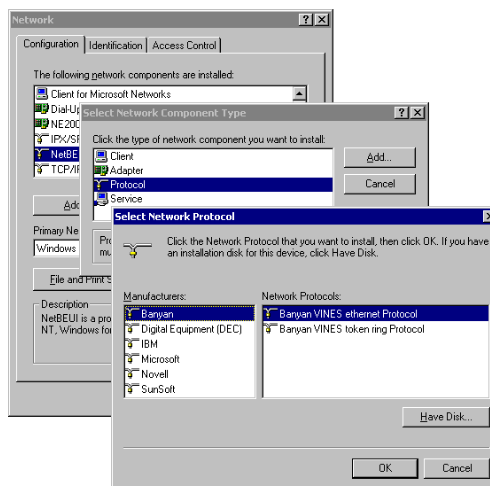
הערה: לידיעתך, SNA Server של מיקרוסופט הוא מוצר המתוכנן לקישוריות הדדית של רשתות מחשבים אישיים עם רשתות SNA, כמו אלו המשמשות מחשבים גדולים ומחשבי AS/400 של יבמ.

X-Windows

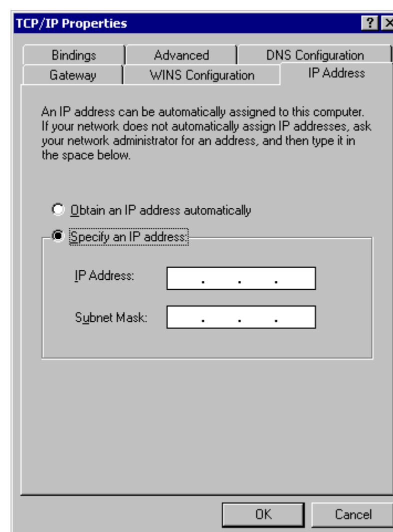
X-Windows היא מערכת פרוטוקולים שפותחו על ידי MIT לאספקת ממשק גרפי למשתמש עבור תחנות עבודה Unix.

הגדרת תצורת פרוטוקולים

בעת ההגדרה הראשונית של המחשב שלך לרישות, בעת התקנת מערכת ההפעלה, או בעת התקנה מאוחרת יותר של כרטיס ממשק רשת, תתבקש להתקין פרוטוקולים. חלק ממערכות ההפעלה, כמו Windows NT, מתקינות עבורך אוטומטית פרוטוקולי רשת. אם ברצונך להתקין פרוטוקולים נוספים מאוחר יותר, בדרך כלל תוכל להשתמש בממשק גרפי כמו זה המוצג בתרשים 8.1. במערכות הפעלה של מיקרוסופט, יכולת זו נמצאת באובייקט **רשת** (Network) ש**בלוח הבקרה** (Control Panel).



תרשים 8.1: *Windows 9x מאפשרת התקנה פשוטה של פרוטוקולי רשת נוספים באמצעות תיבת הדו-שיח Select Network Protocol (בחר פרוטוקול רשת)*



תרשים 8.2: *Network Control Panel מאפשר הגדרת פרוטוקולי רשת באמצעות תיבות דו-שיח מתאימות, כפי שמוצג בדוגמת תיבת הדו-שיח TCP/IP Properties*

ממשק גרפי זה מספק גם מנגנון להסרת פרוטוקולים ולהגדרות. במערכות הפעלה של מיקרוסופט, בדרך כלל ניתן ללחוץ לחיצה כפולה על שם פרוטוקול הרשת, כדי להגיע לאפשרויות ההגדרה הנוספות (ראה תרשים 8.2).

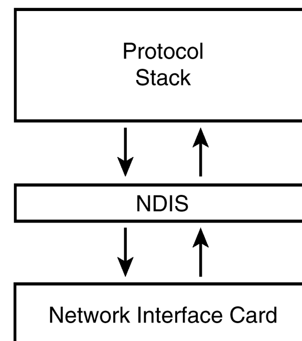
התפקידים של NDIS ו- ODI

כאשר רשתות מחשבים פותחו לראשונה, כל דרייבר רשת וכל כרטיס ממשק רשת יכלו להתקשר (**Bound**) למחסנית פרוטוקול אחת בלבד. מצב זה התאים לרשתות ראשוניות שהשתמשו בפרוטוקול אחד בלבד. ככל שהרשתות התרחבו והחלו להשתמש במספר פרוטוקולים, צריך היה למצוא פתרון לקישור (**binding**) אל מספר פרוטוקולים. העובדה שרק פרוטוקול אחד בלבד היה קשור לכרטיס ממשק רשת כלשהו, השפיע במיוחד על שרתים שהיו צריכים לתקשר עם כל תחנות העבודה, הלקוחות. ניתן היה לפתור את הבעיה על ידי התקנת מספר כרטיסי רשת וקישור כל אחד מהם לפרוטוקול יחיד, אולם פתרון זה לא היה רצוי.

במקום זאת, פותחו driver interfaces שאפשרו לקשור מספר פרוטוקולים לכרטיס ממשק רשת יחיד. שני תקנים שונים (בלתי תואמים) עבור ממשקי דרייבר נמצאים כיום בשימוש:

- ✯ Open Driver Interface (**ODI**). פותח על ידי Novell ו-Apple. ODI נמצא בעיקר ברשתות Novell NetWare.
- ✯ Network Driver Interface Specification (**NDIS**). פותח על ידי מיקרוסופט. NDIS משמש בעיקר ברשתות המשתמשות במוצרי רישות של מיקרוסופט.

כפי שמוצג בתרשים 8.3, NDIS מקשר בין הפרוטוקול בשימוש (TCP/IP או IPX/SPX) לכרטיס הרשת.



תרשים 8.3: *NDIS מאפשר למספר פרוטוקולים לפעול עם אותו כרטיס ממשק רשת*

> **רעיון מפתח**
>
> NDIS ו-ODI מאפשרים למספר מחסניות פרוטוקול להשתמש באותו כרטיס ממשק רשת.

תרגום שמות NetBIOS

כפי שהוזכר בתחילת הפרק, NetBIOS מספק ממשק תכנות יישומים (API) בשכבות עליונות שבו משתמשים היישומים כדי לתקשר עם משאבי הרשת. מכיון שרוב יישומי Windows משתמשים ב-API של NetBIOS, חיוני שתבין כיצד שמות NetBIOS מתורגמים לכתובות רשת (NetBios Name Resolution).

כפי שכבר הוזכר, NetBIOS מזהה כל מחשב ברשת באמצעות שם בן 15 תווים, כאשר תו נוסף משמש לאספקת מידע מערכת אודות השם. שם NetBIOS נוצר בדרך כלל בעת ההתקנה הראשונית של מערכת ההפעלה במחשב, או בעת הפעלת תוכנת הרישות. עם ההפעלה הראשונה של מחשב, הוא משדר את שמו אל הרשת. אם קיים שם זהה, המשתמש או המנהל יצטרכו לשנות את שם NetBIOS של המחשב לפני שמחשב זה יוכל להשתמש במשאבי הרשת.



הערה: אם תרצה לראות את כל שמות NetBIOS המוקצים למחשב Windows 9x/NT/2000, הקלד את הפקודה **nbtstat -n** בשורת הפקודה. כדי שפקודה זו תבצע את הנדרש, המחשב חייב להשתמש בפרוטוקול רשת TCP/IP.

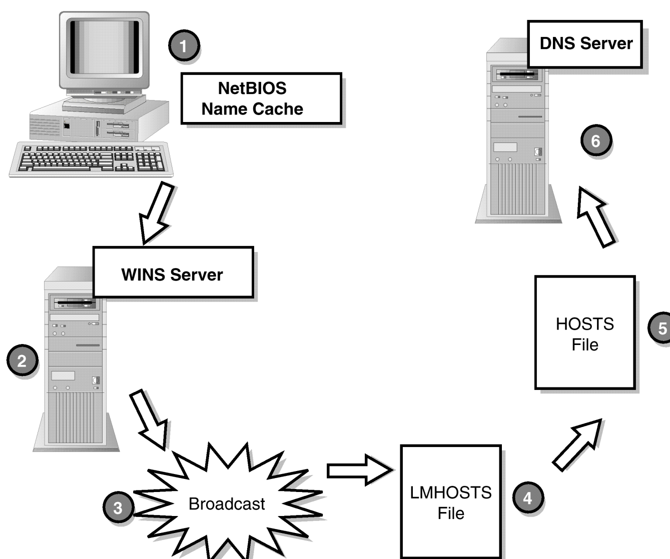
כאשר מחשב רוצה להתקשר למחשב אחר ברשת באמצעות NetBEUI, NetBIOS בודק תחילה מטמון שמות מקומי, כדי לדעת אם כתובת החומרה מוכרת לו. אם לא, NetBIOS שולח שידור חסר-קישור (Connectionless Broadcast) לכל המחשבים ומחפש מחשב בעל שם נתון. כאשר מחשב היעד מגיב עם כתובת החומרה שלו, נוצרת שיחת NetBIOS בין שני המחשבים.

לעומת זאת, במחשב המשתמש ב-TCP/IP, איתור מחשבים אחרים אינו פשוט כל כך. מכיון שרשתות TCP/IP משתמשות בכתובות רשת (IP Address) לחיבורי רשת, NetBIOS חייב לעטוף בקשות למשאבים במנות TCP/IP בעזרת פרוטוקול NetBIOS over TCP/IP (NBT). בנוסף, רשתות TCP/IP מורכבות בדרך כלל ממספר מקטעי רשת המחוברים יחד באמצעות **נתבים** (routers). מכיון ש-NetBIOS משתמש בעיקר בשיטת Broadcast כדי לתרגם שמות ומכיון שמרבית הנתבים אינם Broadcast packets, יש צורך בשיטות חלופיות לתרגום שמות.

ברשתות TCP/IP, NetBIOS משתמש בהיררכיה הבאה לתרגום שמות רשת לכתובות IP (מוצג גם בתרשים 8.4). זהו למעשה סדר החיפוש של שם נתון :

1. מטמון שמות NetBIOS
2. שרת WINS (אם מוגדר)
3. שידור לכל (NetBIOS Broadcast)
4. קובץ LMHOSTS (אם אפשרי)
5. קובץ HOSTS (אם נמצא)
6. שרת DNS (אם מוגדר)

בשעה שמטמון שמות NetBIOS ושידור לכל NetBIOS הן השיטות שהוזכרו, השיטות האחרות דורשות הסבר נוסף.



תרשים 8.4: *מערכות הפעלה של מיקרוסופט מתרגמות שמות NetBIOS במספר דרכים*

WINS

Windows Internet Name System (WINS) הוא שירות של Windows NT המספק תרגום דינמי של שמות NetBIOS לכתובות IP. כאשר מחשב המוגדר להשתמש ב-WINS מופעל, המחשב מתקשר לשרת WINS עם שם NetBIOS וכתובת IP שלו. שרת WINS מוסיף את הצירוף שם/כתובת למסד הנתונים שלו, ולעיתים אף מעביר מידע זה לשרתי WINS נוספים ברשת התקשורת המקומית. כשמחשב הפועל עם WINS צריך להתקשר למחשב אחר ברשת, NetBIOS יוצר קשר עם שרת WINS לבירור כתובת הרשת של מחשב היעד.

מכיון ש-NetBIOS הוא חסר-ניתוב, בקשות **שידור לכל** (Broadcast) של NetBIOS מגיעות למחשבים ברשת המקומית בלבד. לכן, כשמחשב ללא WINS מנסה ליצור קשר עם משאב רשת, NetBIOS יראה רק את המחשבים ברשת המקומית. אולם, לאחר שמחשב מוגדר לעבוד עם WINS, NetBIOS יראה את השמות וכתובות הרשת של כל המחשבים האחרים שנרשמו עם שרת WINS, ללא תלות במקטע הרשת בו הם נמצאים. כך, שרת WINS יכול לאפשר לכל המחשבים לראות את כל המחשבים האחרים, כאילו היו ברשת המקומית.

הדבר דומה לשירות מודיעין 144. אם ברצונך ליצור קשר עם אדם ואינך יודע את מספר הטלפון שלו אז אתה פונה למודיעין 144. שם מאתרים עבורך את המספר ויוצרים את הקישור.

קובץ LMHOSTS ו-HOSTS

בתקופה שקדמה לשירותי WINS, השיטה העיקרית עבור תרגום כתובות NetBIOS לכתובות IP היתה באמצעות רשומות בקובץ LMHOSTS או HOSTS. קבצים אלה היו קבצי טקסט פשוטים שתוחזקו ידנית, ובהם היו רשומות כתובות IP ולאחריהן שמות NetBIOS. בעוד שניתן להשתמש בקבצים אלה לתרגום שמות גם היום, השילוב של WINS ו-DNS מספק את תרגום השמות הדרוש.

הדבר דומה לספר טלפונים הנמצא בהישג ידך ובעזרתו ניתן לאתר את מספרי הטלפון.

DNS

Domain Name System (DNS) משתמש במערכת מבוזרת של שרתי שמות למיפוי **שמות תחום** (domain names) בסגנון אינטרנט, כגון **microsoft.com**, לכתובות IP תקפות. אם NetBIOS אינו יכול למצוא את כתובת IP של שם רשת בכל אמצעי אחר, NetBIOS יפעיל שאילתה על שרת DNS.

סיכום

כשם שפרוטוקולים בינלאומיים מגדירים כיצד צריכה להתרחש תקשורת בין אנשים זרים, פרוטוקולי רשת מגדירים כיצד תקשורת צריכה להתרחש בין מחשבים.

בדרך כלל פרוטוקולי תקשורת מחשבים מקובצים ל**מחסנית פרוטוקול** (protocol stack) או **מערכת פרוטוקול** (protocol suite) ומותקנים במחשב כדי שיוכל להתקשר לרשת. שתי מחסניות הפרוטוקול הנפוצות ביותר הן TCP/IP המשמשת באינטרנט ו-IPX/SPX של Novell המשמשת ברשתות Novell NetWare.

לפרוטוקולים יש תכונות ומאפיינים רבים, אולם שניים שמאפשרים אבחנה בין פרוטוקולים שונים הם סוג החיבור והיכולת להיות מנותב. פרוטוקולים **מוכווני-קישור** (connection-oriented) מספקים חיבור נקודה-לנקודה אמין המבטיח משלוח נכון של נתונים. פרוטוקולים **חסרי-קישור** (connectionless) שולחים את הנתונים ליעדם ללא כל בדיקה שאכן הגיעו אליו. פרוטוקולים **מנותבים** (routable) מתאימים לרשתות החל מרשתות משרדיות קטנות וכלה ברשתות גדולות של החברה כולה, ואילו פרוטוקולים **חסרי-ניתוב** (non-routable) מיועדים בעיקר לרשתות קטנות.

שלוש מחסניות פרוטוקול מקובלות מאוד ברשתות מערכות הפעלה של מיקרוסופט:

- TCP/IP,
- IPX/SPX,
- ו-NetBEUI.

מערכת פרוטוקולי TCP/IP התפתחה במקביל לפיתוח האינטרנט ונמצאת כיום בשימוש נרחב ברשתות מכל הגדלים. המערכת כוללת מספר פרוטוקולים, שהחשובים שבהם כוללים את **IP** (Internet Protocol) המספק תעבורת נתונים, ואת **TCP**

‏(Transmission Control Protocol) המספק תעבורת נתונים אמינה מוכוונת-קישור על פני IP.

כדי לתקשר ברשתות TCP/IP, מוקצית לכל מחשב כתובת IP ייחודית בת 32 סיביות (IP address) המורכבת מחלק המזהה את הרשת וחלק המזהה את המחשבים ברשת, הנקראים **מארחים** (hosts). מחשבים משתמשים **במסכת רשת-משנה** (subnet mask) כדי לקבוע איזה חלק מכתובת IP מתייחס לרשת ואיזה חלק מתייחס למחשב מסוים. כתובות IP מוקצות ידנית או מסופקות באופן דינמי באמצעות פרוטוקול **DHCP** (Dynamic Host Configuration Protocol). DHCP מקל על ניהול הרשת ומאפשר העברה פשוטה של מחשבים ממקום למקום בתוך הארגון.

מערכת פרוטוקולי **IPX/SPX** מיועדת בעיקר לרשתות Novell NetWare. כמו ב-TCP/IP, המערכת כוללת מספר פרוטוקולים. בדומה ל-IP, גם IPX (Internetwork Packet Exchange) מספק העברת נתונים בסיסית ברשת, ואילו SPX (Sequenced Packet Exchange), כמו TCP, מספק תקשורת מוכוונת-קישור אמינה.

מיקרוסופט ויבמ פיתחו במשותף את **NetBIOS** (Network Basic Input Output System) ואת **NetBEUI** (NetBIOS Extended User Interface) לתמיכה בתקשורת ברשתות קטנות עד בינוניות. למרות ש-NetBIOS ו-NetBEUI פותחו לעבוד במשולב, הם הופרדו וכיום NetBIOS יכול לפעול עם פרוטוקולים מסוגים שונים.

NetBIOS מספק ממשק תכנות יישומים בשכבת המושב שבו יישומי מחשבים אישיים יכולים להשתמש כדי לגשת למשאבי הרשת. ניתן כיום להשתמש ב-NetBIOS ברשתות TCP/IP ו-IPX/SPX. NetBEUI הוא פרוטוקול קטן, מהיר וחסר-ניתוב המיועד לשאת עליו את NetBIOS ונמצא בעיקר ברשתות קטנות של מחשבים אישיים.

בעוד ש-TCP/IP, IPX/SPX ו-NetBEUI הם הפרוטוקולים העיקריים הפועלים ברשתות מחשבים אישיים, קיים מספר רב של פרוטוקולים נוספים, ביניהם DECnet, DLC, NFS, OSI ו-SNA.

במרבית מערכות ההפעלה כיום מבוצעת התקנת הפרוטוקולים בדרך כלל באמצעות ממשק גרפי למשתמש. ההתקנה מסתייעת בשני ממשקי דרייבר, **NDIS** (Network Driver Interface Specification) ו-**ODI** (Open Driver Interface), המאפשרים קישור (binding) מספר פרוטוקולים לכרטיס ממשק רשת (NIC) יחיד.

לבסוף, מכיון שמרבית יישומי המחשבים האישיים משתמשים ב-NetBIOS לגישה למשאבי רשת, חייבת להיות שיטה כלשהי לתרגום או "פתרון" שמות מחשבים ב-NetBIOS לכתובות רשת תקפות. במקטע רשת מקומי (local network segment), NetBIOS משתמש במנות **שידור לכל** (broadcast packets) לזיהוי מחשבים אחרים. אך מכיוון ש-NetBIOS הוא חסר-ניתוב, יש להשתמש במנגנון מסוים המאפשר למחשבים במקטעי רשת אחרים להכיר זה את זה. המנגנון העיקרי המשמש לכך ברשתות מיקרוסופט הוא **WINS** (Windows Internet Name System), הפועל ברשת TCP/IP ומאפשר לכל מקטעי הרשת לראות שמות NetBIOS כאילו כל המחשבים נמצאים ברשת אחת גדולה. ניתן גם להגדיר ידנית שמות NetBIOS באמצעות קבצי HOST או באמצעות **DNS** (Dynamic Name System).

9

מערכות הפעלת רשת

מערכות הפעלת רשת (network operating systems) מספקות את הדבק המקשר יחד את כל מרכיבי הרשת. פרק זה יסביר את הפונקציונליות של מערכות הפעלת הרשת ואת רכיבי התוכנה הדרושים כדי שרשת תפעל. עד סוף פרק זה תוכל:

- להסביר את תפקודי (functions) מערכת הפעלת הרשת,
- לזהות את רכיבי תוכנת הלקוח,
- לזהות את רכיבי תוכנת השרת,
- לתאר את תהליך ההדפסה ברשת.

תפקודי מערכת הפעלת הרשת

במחשב אישי, **מערכת ההפעלה** (operating system) מטפלת באינטראקציה בינך לבין התוכנה והחומרה. בעוד שמערכות הפעלה מסורתיות כמו DOS ו-Windows בגירסה 3.X מספקות פונקציונליות זו למחשבים בודדים, הן לא תוכננו עם פונקציות רישות כלשהן. עם הזמן, הוספו מספר פעולות רישות מינימליות, אך DOS ו-Windows עדיין מיועדות בעיקרון לשימוש על מחשבים אישיים בודדים.

לעומת זאת, **מערכת הפעלת רשת - NOS** (Network Operating System) מתוכננת לספק את כישורי הרישות הדרושים לפעילות הרשת. מערכת הפעלת רשת, כדוגמת Novell NetWare או Windows NT/2000, פועלת בדרך כלל על מחשב **שרת** (server), בזמן שמערכת הפעלה רגילה, כמו Windows 9x/ME או Windows NT Workstation או Windows 2000 Professional או DOS, פועלת על מחשבי **לקוח** (client).

כיום, הבחנה זו היטשטשה עם מערכות הפעלה כמו Windows NT Workstation, Windows 2000 Professional ו-Windows 9x/ME, אשר מיועדות כולן למחשבי לקוח, אולם מספקות מספיק תפקודי רישות ולכן אפשר לראות גם אותן כמערכות הפעלת רשת.



הערה: מילה על מערכת ההפעלה Windows. **לחברת** Microsoft **שני "קווים"** של מערכות הפעלה:

- ✯ **מערכת הפעלה ביתית ו/או לעסק הקטנטן הכוללת את** Windows 95, Windows 98, Windows ME,
- ✯ **מערכת הפעלה** Windows NT **ו-** Windows 2000.

במערכות אלה יש מערכת הפעלה:

- ✯ **לקוח (**Client**) שב-**Windows NT **הוא נקרא** Workstation **וב-**Windows 2000 **הוא נקרא** Professional.
- ✯ **שרת הנקרא** Windows NT Server **ו-** Windows 2000 Server.

זה לא הכל, לכל מערכת (כמעט) יש גירסאות משנה כמו Windows 98 **ו-** Windows 98 Second Edition.

ויש גם "מוטציות", למשל Small Business Server **זה למעשה** Windows NT **בגירסה לעסקים קטנים ובינוניים. למערכת** Windows 2000 **יש סדרה שלמה של שרתים, למשל** Windows 2000 Advanced Server **ו-** Windows 2000 Datacenter Server.

למערכת הפעלת רשת מספר תפקידים חשובים:

- ✯ שיתוף קבצים ומדפסות,
- ✯ ניהול חשבונות משתמשים,
- ✯ אבטחת רשת.

כדי שפעולות אלו יתקיימו, יש להתקין תוכנה מתאימה על מחשבי הלקוח ועל שרתי הרשת.

רכיבי תוכנה

ברשת מחשבים יש להתקין שני רכיבי תוכנה:

- ✯ **תוכנת לקוח** (client software), המאפשרת למשתמשים לגשת ולהשתמש במשאבי הרשת, כמו שרתי קבצים ומדפסות.
- ✯ **תוכנת שרת** (server software), המאפשרת למחשב לספק למחשבים אחרים גישה למשאבי הרשת, בנוסף לביצוע פעולות ניהול אחרות.

שני סוגי התוכנה השונים יידונו בהמשך.

תוכנת לקוח (Client Software)

במחשב בודד (stand alone), בקשות לקובץ או למשאבי הדפסה מטופלות על ידי המעבד (CPU). לדוגמה, כאשר משתמש במחשב בודד מבקש לראות את רשימת התיקיות, כפי שמוצג בתרשים 9.1, בקשתו מטופלת על ידי המעבד במחשב המקומי.

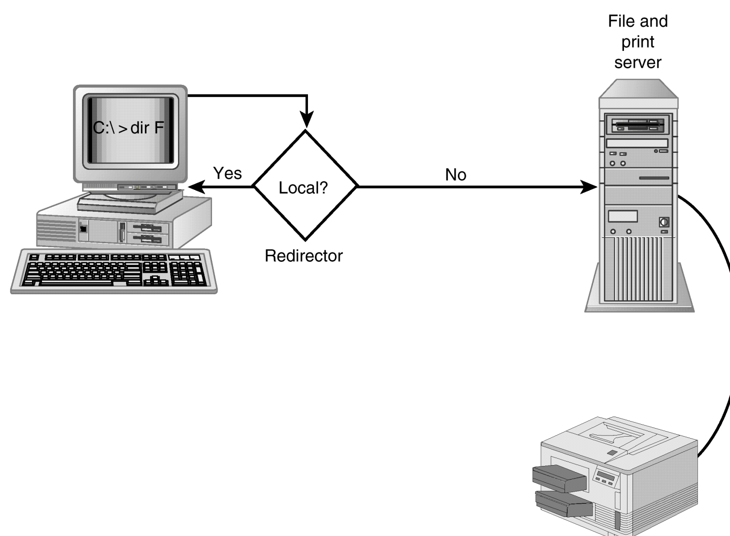


תרשים 9.1: *בקשת משתמש להציג רשימת תיקיות במחשב בודד מטופלת על ידי המחשב המקומי*



הערה: מערכות Windows 9x/NT/2000 משתמשות במונח **תיקיה** (folder) במקום המונח **ספריה** (directory) המשמש ב-DOS, ב-Windows 3.x ובו-Windows NT 3.51. בהמשך הספר יוזכרו שני מונחים אלה כשווים.

לאחר התקנת תוכנת רישות על המחשבים, נכנסת לתמונה **תוכנת ניתוב** (redirector). תוכנת הניתוב מקבלת את כל הבקשות לקבצים או למשאבי הדפסה וקובעת אם הן מיועדות למחשב המקומי או למשאב מקומי, היא מועברת למעבד. אם הבקשה מיועדת למשאב רשת, תוכנת הניתוב מעבירה אותה לשרת הרשת המתאים, כפי שמוצג בתרשים 9.2.



תרשים 9.2: *בקשת משתמש לרשימת ספריות של מחשב ברשת מטופלת על ידי תוכנת ניתוב (redirector)*

היתרון בגישה זו הוא שמיקום המשאבים שקוף ליישומים שלך. כאשר אתה עובד ביישום כלשהו ושומר את הקובץ בכונן מסוים, היישום אינו חייב לדעת אם כונן זה נמצא במערכת המקומית, או בשרת קבצים כלשהו ברשת. **תוכנת הניתוב גורמת למחשב לראות את כל הכוננים כאילו היו מקומיים**. באופן דומה, כאשר אתה בוחר להדפיס קובץ, היישום שלך שולח בקשת הדפסה למדפסת שבחרת. תוכנת הניתוב מפנה בקשה זו אל המדפסת המתאימה המקומית, או לזו שברשת.

בסביבת מחשבים אישיים, חלק מהמשימה של תוכנת הניתוב היא לעקוב אחר **מצייני כונן** (drive designators) המסמנים כל משאב ברשת. לדוגמה, למרבית המחשבים יש כונן דיסקטים המסומן ב- :A וכונן דיסק המסומן ב- :C. כאשר אתה רוצה לגשת לנתונים שבספריית שרת הקבצים ברשת, אתה **ממפה** (map) לכונן/תיקיה הרחוקה אות כונן, כגון :F או :G. תוכנת הניתוב זוכרת איזה מיפוי יצרת ומאפשרת לך להתייחס אליהם כאילו היו כוננים מקומיים.

מערכות הפעלה כגון Windows 9x/NT/2000 מאפשרות גישה למשאבי רשת משותפים על ידי שימוש בשם UNC (Universal Naming Convention). שם UNC מורכב משם השרת ושם המשאב המשותף (תיקיה, כונן, או מדפסת) ומקבל את הצורה הזו: \\servername\pathname.

לדוגמה, אם תיקיה משותפת בשם MARKETING נמצאת בשרת שנקרא SALESSRVR, שם UNC עבור תיקיה זו יהיה \\SALESSRVR\MARKETING (שים לב ששמות UNC באנגלית **אינם** רגישים לגודל אות). אם קובץ REPORT.DOC נמצא בתיקיה זו, שם UNC לקובץ זה יהיה \\SALESSRVR\MARKETING\REPORT.DOC.



רעיון מפתח

שם נתיב UNC (Universal Naming Convention) הוא דרך התייחסות למשאבי רשת משותפים. תצורת שם UNC היא \\servername\pathname.

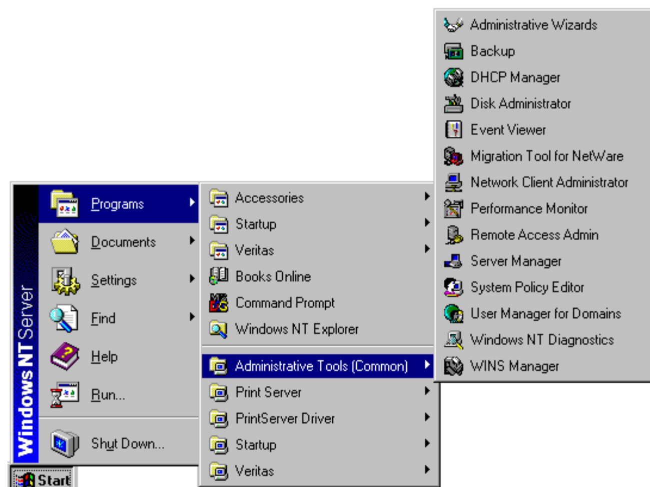
שים לב שבמסגרת התיאורטית של מודל ייחוס OSI, תוכנת הניתוב פועלת בשכבת התצוגה (presentation). ניתן לראות זאת כאילו היא מציגה בקשות משאבים מהיישומים לפרוטוקולי הרישות, ומציגה את משאבי הרשת ליישומים, כאילו המשאבים היו מקומיים.



הערה: תוכנת הלקוח לרשת ברשתות מיקרוסופט נקראת redirector. ברשתות Novell תוכנה זו נקראת requestor.

תוכנת שרת (Server Software)

לקוחות רשת זקוקים לתוכנת הניתוב בלבד, כדי לגשת למשאבי הרשת. לעומתם, שרתי רשת זקוקים לתוכנה מורכבת יותר לביצוע משימותיהם. בדרך כלל, התוכנה הדרושה ארוזה ב**מערכת הפעלת הרשת** - **NOS** (Network Operating System) ומנוהלת באמצעות מיגוון כלי הניהול המסופקים איתה (ראה תרשים 9.3).



תרשים 9.3: *Windows NT כוללת כלים לביצוע משימות ניהול*

לדוגמה, מערכת הפעלת הרשת תספק תוכנה המאפשרת לתיקיות (הנקראות גם ספריות) להיות **משותפות** (shared) ברשת. התוכנה תטפל בנושאים שונים למשל אילו משתמשים יכולים לגשת לתיקיה, כמה משתמשים יכולים לגשת לתיקיה בו-זמנית, ואילו **הרשאות** (permission) יהיו לכל משתמש לשינוי פריטים בתוך התיקיה.

כחלק מתהליך זה, תוכנת שרת גם מטפלת בבקשות נכנסות מתוכנות ניתוב שבמחשבי לקוח ושולחת בקשות אלו למשאב המתאים.

תוכנת שרת מספקת גם כלים לניהול חשבונות משתמשים ולאבטחת רשת. לפני התחברות למשאבי רשת המשתמש חייב להיכנס (logon או login) לרשת. הכינוי באנגלית נובע מכך שהוא מקליד (רושם) שם או כינוי. מערכת הפעלת הרשת מנהלת תהליך כניסה זה, וקובעת אם המשתמש יוכל לגשת למשאבי הרשת. כלי הניהול מאפשרים למנהלי הרשת להוסיף או למחוק משתמשים, ולקבוע את רמת הגישה לרשת שתותר לכל משתמש.

מכיון ששרתים משמשים בדרך כלל לשמירת נתונים חשובים ולמעשה - הנתונים התפעוליים של הארגון, מערכות הפעלת רשת משלבות גם תוכנת גיבוי המאפשרת הגנה נוחה על הנתונים. במקרים רבים תוכנה זו תשמש בשילוב עם כונני דיסק **בעלי סיבולת לתקלות** (fault tolerant) תוספת רמה נוספת של הגנת חומרה. בנוסף, רוב מערכות הפעלת רשת מספקות תוכנה ל**בקרת ביצועי הרשת** (Network Monitor).

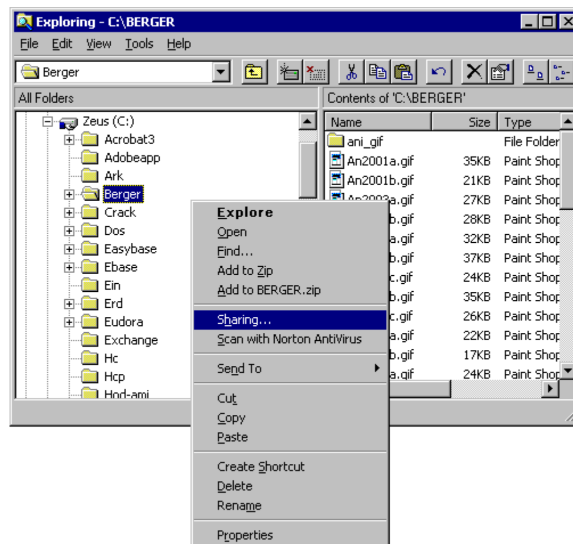
רכיבים אחדים של תוכנת שרת משולבים גם במערכות הפעלת לקוח כמו Windows 9x/NTW/2000 Professional. במערכות אלו, מחשב יכול לגשת למשאבי רשת כלקוח וגם לשתף משאבים שלו עם אחרים כמו שרת. במצב זה, המחשב נקרא שוויוני (peer).

שירותי רשת (Network Services)

מערכת הפעלת רשת מספקת שירותים לרשת כולה החל משירותים למשתמשים, כלים לניהול המערכת, לביצוע גיבויים, אבטחת מידע ועוד.

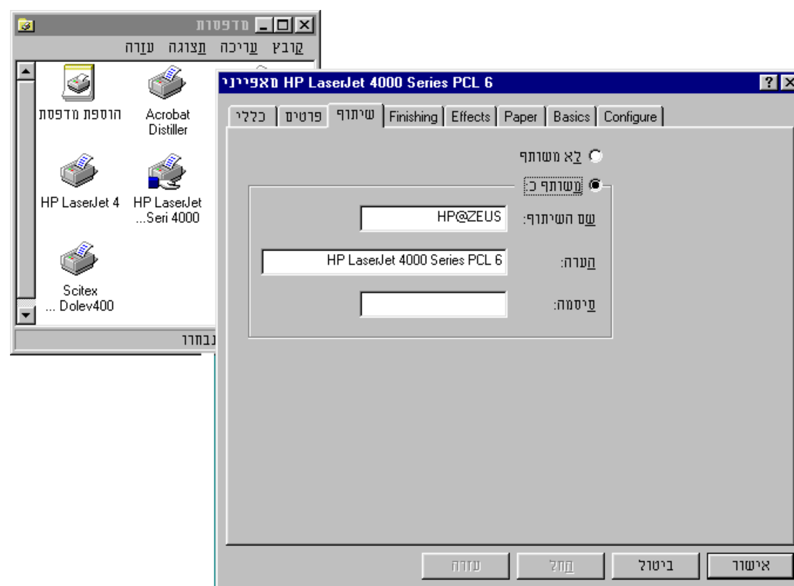
שיתוף קבצים (File Sharing)

שיתוף קבצים הוא הדבר הבסיסי ביותר בכל סוג של רשת. על מנת שמשתמשים אחרים יוכלו לגשת לקבצים הנמצאים בתיקיה בדיסק הקשיח במחשב שלך יהיה עליך לשתף את התיקיה. **שים לב** שאינך יכול לשתף קובץ בודד, אלא לשתף תיקיה (ספריה) המכילה קובץ זה. תוכל לקבוע ת רמת השיתוף של התיקיה: לקריאה בלבד, לקריאה ולכתיבה או גישה מלאה עם סיסמה.



תרשים 9.4: ב-Windows יש ללחוץ על הלחצן הימני בעכבר כדי להציג תפריט שממנו ניתן לפתוח את תיבת הדו-שיח Sharing

באותה צורה ניתן גם לשתף משאבים אחרים כמו מדפסת.



תרשים 9.5: שיתוף מדפסת במחשב לקוח עם מערכת הפעלה Windows

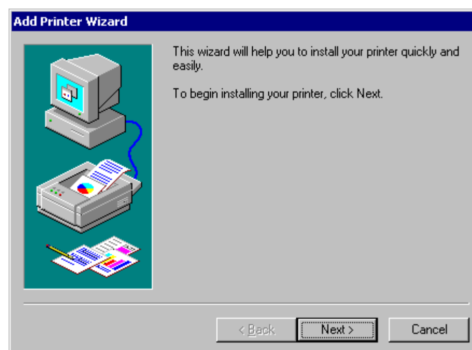
הגישה למשאבים משותפים יכולה להעשות במספר דרכים. אם הכונן ממופה (Map) הרי יש לו אות (כנון S) ואפשר לפנות אליו בשם זה. אם הכונן אינו ממופה אז אפשר לפנות אליו דרך יישום המאפשר סריקה של כל המשאבים המשותפים ברשת. במערכת

הפעלה מסוג Windows ניתן לעשות זאת באמצעות Windows Explorer ובחירה ב-Network Neighborhood (שכנים ברשת).

הדפסה ברשת (Network Printing)

הדפסה ברשת מורכבת מעט יותר משיתוף קבצים, אולם התהליך עצמו של שיתוף מדפסת או חיבור למדפסת משותפת מתרחש באופן דומה מאוד לתהליך שיתוף קבצים או התחברות לקבצים משותפים. כמו בעת שיתוף קובץ, ניתן לקבוע שם למדפסת משותפת ולהקצות הרשאות גישה מתאימות. ההבדל העיקרי הוא שבמקום להשתמש במנהל הקבצים או מנגנון שכנים ברשת, תשתמש במנהל ההדפסה או באובייקט המדפסות שבלוח הבקרה. כדי להתחבר למדפסת שטרם הוגדרה, Windows מאפשרת להפעיל את האשף Add Printer המוצג בתרשים 9.6, המפשט במידה רבה את התהליך.

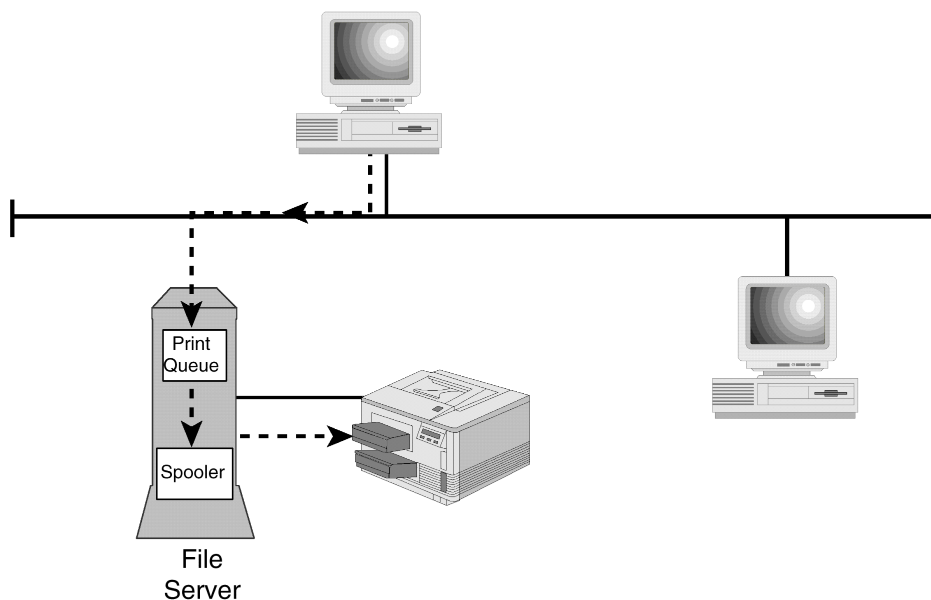
לאחר התחברות כלקוח למדפסת ברשת, תוכנת הניתוב של המחשב תפנה אל המדפסת הזו את כל בקשות ההדפסה שהופנו אליה, בדיוק כפי שהיא מפנה את כל בקשות הקבצים לתיקיה המתאימה.



תרשים 9.6: *אשף Add Printer של Windows מפשט את משימת החיבור למדפסות ברשת*

מורכבות ההדפסה היא בצד השרת. כאשר מגיעה פנייה לשימוש בקובץ הנמצא בתיקיה משותפת, משימת השרת קלה: עליו לקבוע אם הקובץ בשימוש על ידי מישהו אחר ולבדוק אם למבקש יש הרשאה לגשת לקובץ. אם אין בעיה, השרת מחזיר את הקובץ המבוקש. אם יש בעיה, השרת מחזיר הודעת שגיאה.

באופן דומה, כאשר השרת נדרש להדפיס קובץ, הוא קובע אם למבקש יש הרשאה להשתמש במדפסת; ואם לא, הוא מחזיר הודעת שגיאה. אולם, גם אם מותר למשתמש להדפיס את הקובץ, השרת אינו שולח אותו מיידית למדפסת, אלא מעביר את **עבודת ההדפסה** (print job) ל**תור ההדפסה** (print queue) כדי שתבוצע **כהדפסה ברקע** (spooling). הקובץ ממתין בתור עד שהמדפסת תהיה מוכנה להתחיל בהדפסתו (ראה תרשים 9.7). **תוכנית הדפסה ברקע** (spooler) סורקת את התורים ואת מצב המדפסות ומנהלת את תהליך הדפסת המסמכים במדפסת.



***תרשים 9.7:** כאשר קובץ מודפס במדפסת רשת הוא מועבר (spooled) לתור הדפסה (print queue) בו הוא ממתין עד שהמדפסת מוכנה להדפיסו*

תהליך זה מאפשר למספר משתמשים להדפיס למדפסת רשת, מבלי להפריע זה לזה. כל עבודת הדפסה שמגיעה נכנסת לתור עד שתוכנית ההדפסה ברקע מאפשרת לה להמשיך אל המדפסת עצמה. מחשב המתפקד כשרת הדפסה ייעודי יכול להיות מחובר למספר מדפסות, שלכל אחת מהן תור הדפסה נפרד.

תכונה נוספת של מערכת הפעלת רשת היא שבדרך כלל משתמשים יכולים לנהל את תור הדפסה מרחוק. אם משתמשים רוצים לבטל עבודת הדפסה ששלחו למדפסת, הם יכולים לפתוח את מנהל ההדפסה, או את חלון המדפסת הזו ולבטל את הדפסת הקובץ. למרות שבדרך כלל משתמשים מוגבלים לניהול עבודות ההדפסה שלהם בלבד, מנהלי רשת יכולים לנהל מרחוק את כל התור ולבטל עבודות הדפסה של כל אחד, או לשנות את סדר ההדפסה.

דרייברים למדפסת (print drivers) הם המרכיב האחרון במורכבות ההדפסה ברשת. כמו בכרטיסי ממשק רשת, מערכת ההפעלה משתמשת בדרייברים כדי לתקשר עם המדפסות. רצוי לדעת שכל מערכת הפעלה עשויה להשתמש בדרייברים אחרים לאותן מדפסות. לכן מתעוררת בעיה כאשר משתמש במחשב Windows 95 רוצה להדפיס למדפסת משותפת שמחוברת למחשב Windows 2000 Server. מכיון שהדרייברים למדפסת של Windows 2000 Server ו-Windows 95 שונים זה מזה, משתמש Windows 95 לא יוכל סתם כך, להדפיס למדפסת המחוברת למחשב האחר.

קיימים שני פתרונות לבעיה זו. האחד, ניתן לטעון על מחשב השרת את הדרייברים של כל מערכות ההפעלה אשר אמורות להשתמש במדפסת. כך שבסביבת מיקרוסופט אופיינית תטען דרייברים למדפסת עבור Windows 2000, Windows NT, Windows 9x/ME. כך, כל משתמש יוכל להתחבר למדפסת זו ותוכנות הניתוב וההדפסה ברקע יוכלו להשתמש בדרייברים המתאימים. דרך חלופית היא להתקין את הדרייברים המתאימים למדפסות על מחשבי הלקוח. בדרך זו, כאשר משתמש רוצה להדפיס, תוכנת הניתוב מכינה את קובץ ההדפסה על פי הדרייבר הדרוש במחשב שאליו מחוברת המדפסת, לפני העברתו לשרת ההדפסה.

סיכום

מערכת הפעלה רגילה מטפלת בתקשורת שבין משתמש לבין חומרה ותוכנה במחשב. מערכת הפעלת רשת מספקת פונקציונליות נוספת, המאפשרת למשתמשים לשתף קבצים ומדפסות ברשת, לנהל חשבונות משתמשים ולספק אבטחת רשת. מערכות הפעלת רשת נפוצות בעולם המחשבים האישיים הן Windows NT Server ו- Novell NetWare.

מעבר לרכיבים הפיסיים, חיבור מחשב לרשת כרוך בהתקנת רכיבי תוכנה נוספים. בצד הלקוח, תוכנת ניתוב מאפשרת למשתמשים למפות משאבי רשת לאותיות כונן נוספות, ולהשתמש במשאבים אלה כאילו היו כונני דיסק מקומיים. למעשה, תוכנת הניתוב מקבלת כל בקשה לשמירה או אחזור קבצים, קובעת אם הקובץ מקומי או במחשב רשת כלשהו ושולחת אותה למשאב המתאים. מערכות הפעלה אחדות כמו Windows NT ו-Windows 95 כבר כוללות תוכנת ניתוב; במערכות אחרות, כמו DOS ו-Windows 3.1 , יש להתקין אותן בנפרד.

תוכנת שרת כוללת מספר שירותים וכלי ניהול הכלולים מראש במערכות הפעלת רשת כגון Windows NT Server. בדרך כלל תוכנת שרת כוללת כלים לניהול חשבונות משתמשים, גיבוי והגנה על נתונים, ופיקוח על ביצועי הרשת.

רוב מערכות הפעלת רשת מספקות שירותי שיתוף קבצים ושיתוף מדפסות. כדי לשתף קבצים בסביבת מיקרוסופט, ניתן להשתמש בשורת הפקודה, במנהל הקבצים, או בסייר חלונות. ניתן להגדיר הרשאות כדי לקבוע אילו משתמשי רשת יוכלו לגשת לנתונים המשותפים.

למרות ששיתוף מדפסות מושג באופן דומה, תהליך השרת כולל מספר צעדים. כאשר המשתמש שולח משימת הדפסה, היא מועברת לתור הדפסה. תוכנית ההדפסה ברקע בודקת את מצב המדפסות ומאשרת את הדפסת העבודה כשיש מדפסת זמינה. ניתן לנהל מדפסות מרחוק, ומנהלי רשתות יכולים בדרך כלל לבטל, או לשנות סדרי עדיפויות של משימות הדפסה.

10

יישומי רשת

ברמה הבסיסית, רשתות נועדו להקל על העברת קבצים בין מחשבים. אולם, רשתות יכולות לספק הרבה יותר פונקציונליות (תפקודים). בפרק זה תלמד כיצד יישומים יכולים לפעול בסביבה מרושתת ואת היתרונות שהם יכולים לספק לארגון שלך. עד סוף פרק זה תוכל:

- ✯ לתאר כיצד יישום יכול לפעול עם הרשת,
- ✯ לזהות את הסוגים השונים של יישומים לרשת-בלבד,
- ✯ להבין יישומי רשת כגון דואר אלקטרוני, יישומי תזמון (scheduling) ויישומי קובצה או קבוצת עבודה (groupware).

יישומים בסביבה מרושתת

כאשר אתה עובד על מחשב, אתה משתמש בתוכנית, או **יישום** (application) מסוג כלשהו, כדי לבצע את משימתך. לדוגמה, אתה יכול להשתמש במעבד תמלילים, גיליון אלקטרוני, בסיס נתונים, משחק או יישום אחר.

לכל אחד מיישומים אלה יכולות להיות רמות אינטראקציה שונות עם הרשת עצמה, ולכן ניתן לסווג אותם לאחד משלושה סוגים:

- ✯ יישומים עצמאיים (Stand-alone Applications)
- ✯ גרסאות רשת ליישומים עצמאיים (Network versions of Stand-alone Applications)
- ✯ יישומי רשת-בלבד (Network-only Applications)

יישומים עצמאיים

יישומים עצמאיים (stand-alone applications) מיועדים לפעול על מחשב יחיד **בלי צורך** ברשת. דוגמאות לכך הם מעבדי תמלילים מסורתיים כמו Microsoft Word ו- WordPerfect, או גליונות אלקטרוניים, כמו Microsoft Excel או Lotus 1-2-3.

בדרך כלל אינטראקציית רשת עם יישומים מסוג זה מוגבלת לשימוש בקבצים משרת קבצים. לדוגמה, ניתן **לטעון** (mount) או **לצרף** (attach) ספריה משרת הקבצים אל המחשב המקומי, ואז היא תוצג כאות כונן נוספת, למשל "F:". משתמשים ביישומים עצמאיים על מחשב זה יוכלו לשמור קבצים לכונן F:, כאילו היה זה כונן C: או A:. מבחינתם, כונן הרשת אינו שונה מכוננים מקומיים. כך מנהלי הרשת יכולים לנהל ביעילות את משאבי המחשבים בעזרת כונני דיסק גדולים הזמינים לכל המשתמשים.

יישומים עצמאיים יכולים להיות גם מותקנים בשרת קבצים או בשרת יישומים, ומשתמשים יכולים להפעיל את התוכנית מכונן הרשת. לדוגמה, אם לחברה יש עותק אחד של תוכנית מסד נתונים ומספר אנשים צריכים להשתמש בה, ניתן למקם אותה על שרת. כך יוכלו מספר משתמשים להריץ תוכנית זו משרת הקבצים.

שימוש ביישום באופן זה עלול להפר את הרשיון לתוכנה, ולהעמיד את החברה בסיכון משפטי. תגלה גם שקיימים יישומים עצמאיים שאינם פועלים כך, ואינם מאפשרים למספר משתמשים לגשת לתוכנה שמותקנת במחשב אחר.

כדי לאפשר למשתמשים להריץ יישום ברשת, יש להשתמש **בגרסת הרשת** של יישום עצמאי זה (Network Stand Alone Applications).

גרסאות רשת ליישומים עצמאיים

גרסאות רשת ליישומים עצמאיים (network stand-alone applications), למעשה, זהות לגרסאות התוכנה של יישומים עצמאיים, אולם הן **מתוכננות** להיות תואמות לעבודה ברשת, יכולות לנצל תכונות רישות, ובדרך כלל ניתן עליהן רשיון למספר משתמשים בו-זמנית. לאחר התקנת יישום מסוג זה, ייתכן והמשתמשים כלל לא יבחינו בהבדל ביחס ליישום העצמאי שהיה קודם לכן. בסביבת חלונות, הם ילחצו לחיצה כפולה על סמל ויפתחו את היישום כפי שעשו תמיד.

למרות שמשתמשים אולי לא יבחינו בהבדל, יישומים משותפים יכולים להקל מאוד על מנהלי רשת. לפניך כמה מהיתרונות:

- ✯ **התקנה וניהול פשוטים יותר**. יש צורך להתקין רק גירסה אחת של התוכנה, במקום להתקין אותה בנפרד בתחנת העבודה של כל אחד מהמשתמשים. שדרוגים כרוכים בשדרוג של גירסה אחת בשרת בלבד. משתמשים אינם חייבים להיות מעורבים בתוכניות ההתקנה, אלא יכולים להפעיל את התוכנה ולהשאיר את הניהול למנהלים.

* **בקרת גרסאות**. התקנת יישום בשרת פירושה **שכל** המשתמשים ישתמשו באותה גירסה של היישום. אין צורך לחשוש ממצב שבו משתמשים אחדים משתמשים בגירסה 4.0 של מוצר בעוד שאחרים משתמשים בגירסה 7.0.
* **עלות**. רוב גרסאות הרשת של יישום מאפשרות **רישוי אתר** (site licensing) המאפשר למספר מוגדר של משתמשים להשתמש ביישום. רשיון אתר ל-200 משתמשים עולה בדרך כלל פחות מרכישת 200 עותקים עצמאיים של התוכנה.

התקנת גרסת רשת של יישום בשרת כרוכה לעיתים בהתקנת היישום לספריה, ולאחר מכן שיתוף הספריה לגישה של אחרים. בדרך כלל נדרשת התקנה של מספר קבצי מערכת בתחנת העבודה המקומית, אך מרבית הקבצים הדרושים נשארים בשרת הקבצים. לרוב, מתקינים יישומים בשרת קבצים יחד עם ספריות המכילות נתונים. לעיתים, מגדירים **שרת יישומים** (application server) למטרת שיתוף יישומים בלבד.

למרות ששיתוף יישומים עשוי להוות יתרון גדול, יש לכך גם מספר חסרונות:

* **מהירות רשת**. יישומים משותפים דורשים רוחב פס תקשורת רחב יותר מאשר יישומים עצמאיים. כאשר למשתמשים יש יישומים עצמאיים, תעבורת הרשת היחידה שהם מייצרים היא תוצאת אחזור קבצים. אולם בגישה לגרסאות רשת של התוכנה, יש להעביר ברשת את כל רכיבי התוכנה של היישום וגם את קבצי הנתונים. שימוש רב ביישומים עלול להאט את הרשת.
* **שיתוק במקרה של תקלה ברשת**. כאשר פועלים ביישומים עצמאיים ויש תקלה ברשת, המשתמשים אינם יכולים לגשת לקבצים השמורים בשרת הקבצים, אך הם עדיין יכולים להפעיל את היישום על קבצים מקומיים. לעומת זאת, בעבודה ביישומים משותפים, תקלה ברשת מונעת מהמשתמשים שימוש כלשהו ביישום.

יישומי רשת בלבד

שיתוף יישומי משרד אופייניים, למשל מעבדי תמלילים, משרת מרכזי נפוץ למדי ברשתות משרדיות ואחרות. עם זאת, קיימים יישומים המתפקדים בסביבה מרושתת בלבד, כי תוכננו לכך מראש. דוגמאות ל**יישומי רשת בלבד** (network-only applications):

* דואר אלקטרוני,
* תזמון קבוצתי (group scheduling),
* קובצה (groupware),
* מסדי נתונים משותפים.

לפני שנדון בדוגמאות אלו, עליך להבין שקיימים מספר מודלים לאופן הפעולת יישומי רשת אלה:

- ✯ **יישומים מרכזיים** (centralized applications),
- ✯ **יישומי מערכת-שיתוף-קבצים** (shared-file-system applications),
- ✯ **יישומי שרת/לקוח** (Client/server applications).

הבנת המודלים השונים חיונית להבנת פעולת יישומי רשת שונים ולאיתור בעיות בהם.

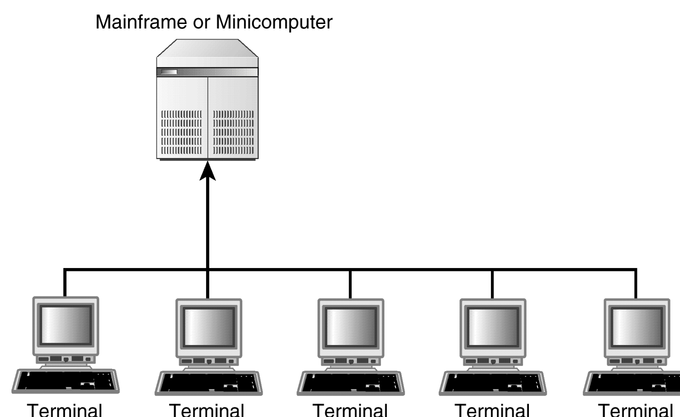
יישומים מרכזיים

תהליך העיבוד מתבצע במחשב המארח-מרכזי, Terminal ← Mainframe.

סביבת **יישומים מרכזיים** (centralized applications) מוצגת בתרשים 10.1. על פי מודל פעילות זה, משתמשים מתחברים למחשב מארח מרכזי גדול (mainframe) באמצעות **מסוף** (terminal) ייעודי, או על ידי פתיחת **מושב מסוף** (terminal session) במחשב האישי שלהם. במצב השני, המחשב האישי מבצע **אמולציה** או חיקוי של עבודת המסוף הרגיל. בכל מקרה, משתמשים רואים מסך או חלון המציג מידע מהמחשב המרכזי. מחשב זה עוסק בכל העיבוד, בשעה שהדו-שיח של המשתמשים עם התוכנית נעשה דרך חלון זה. בדרך כלל תוכניות מסוג זה הן **מבוססות טקסט** (character based) וכוללות גרפיקה מינימלית.

כדוגמה, חשוב כיצד תוכניות מסדי נתונים מסורתיות רבות פועלות במחשבים מרכזיים. למשתמשים יש חלון מסוף המאפשר להם להקליד בקשות למידע. כאשר משתמש מקליד מידע, כל הקשות המקלדת מועברות למחשב המרכזי לעיבוד; כלומר, הוא ממלא פרטים בתבנית טופס כלשהי ושולח זאת אל המחשב. המחשב המרכזי מעבד את הבקשה, מוצא את המידע הדרוש, מגדיר את כל המידע לתצוגה בחלון המסוף ושולח הכל אל המשתמש. שים לב שהמחשב האישי או המסוף שברשות המשתמש אינם משתתפים בכל מהלך הפעולה.

החסרון הוא שיישומים מסוג זה יוצרים תעבורת רשת רבה, אינם מנצלים ביעילות את היכולות של המחשבים האישיים וברגע שהמחשב הראשי "נופל", כל המחשבים (ולמעשה מסופים) מפסיקים לתפקד. לכן, יישומים מרכזיים מוחלפים בהדרגה ביישומי שרת/לקוח (Client/Server).



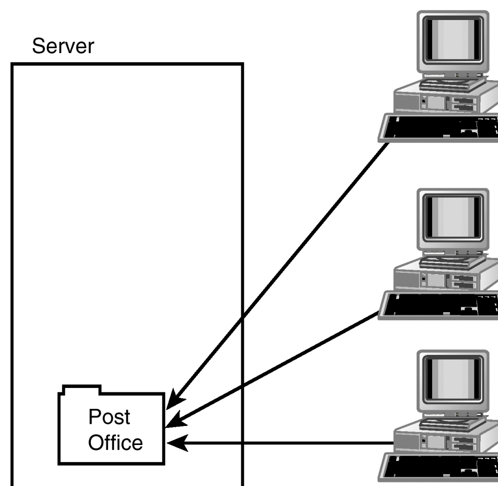
תרשים 10.1: *יישומים מרכזיים מסתמכים על מחשב מארח מרכזי לביצוע העיבוד*

יישומי מערכת-שיתוף-קבצים

תהליך העיבוד מתבצע במחשב האורח-לקוח. בניגוד ליישומים המרכזיים, **יישומי מערכת-שיתוף-קבצים** (Shared-File-System Applications) מבצעים את כל העיבוד במחשב הלקוח, שהוא מחשב אישי, ומשתמשים בשרת לאחסון קבצים בלבד. דוגמה לכך הן תוכנות הדואר האלקטרוני הנפוצות למחשב האישי כגון Microsoft Mail, או cc:Mail. תוכנות מסדי נתונים רבות הפועלות במחשב האישי, מנהלי מידע אישיים - **PIM** (Personal Information Managers), ותוכניות **תזמון** (scheduling) רבות פועלות גם הן לפי מודל זה.

לדוגמה, ברוב תוכנות הדואר האלקטרוני למחשב האישי, נמצא שישנו מחשב מרכזי שבו מאוחסן "משרד דואר". כפי שמוצג בתרשים 10.2, משתמשי מחשבים אישיים משתמשים בתוכנית דואר כדי להגיע ברשת אל הנמענים שהם רוצים בהם, או כדי לאחזר מידע מספריה מסוימת בשרת הקבצים.

חסרון: למרות שמודל מחשוב זה מנצל ביעילות רבה יותר את העוצמה והאפשרויות שבמחשבים האישיים, הוא אינו פותר בהכרח את בעיית התעבורה ברשת. כאשר משתמש מתחיל את תוכנית הדואר וניגש לתיבת הדואר הנכנס שלו, תוכנית הדואר צריכה להעביר את קובץ "הדואר" שלו משרת הקבצים (בדרך כלל) אל קובץ זמני במחשב האישי. כלומר, היא מעבירה "חלק" של משרד הדואר הרלוונטי למבקש. היא גם חייבת לשמור על תיאום בין הקובץ שהועבר לבין שאר הקבצים, באמצעות בדיקות שגרתיות ב"משרד הדואר" שנמצא בשרת הקבצים. גם אם המשתמש מקבל דואר רק לעיתים רחוקות, תוכנית הדואר חייבת להמשיך ולבדוק אם הגיע אליו דואר. תהליך בדיקה זה נקרא **הזמנה לשידור** (polling). תהליך ההזמנה לשידור והעברת הודעות דואר לקבצים זמניים על פני הרשת עשויים ליצור תעבורת רשת רבה.



תרשים 10.2: *תוכנות דואר אלקטרוני המשתמשות במודל מערכת-שיתוף-קבצים מאפשרות למערכות לקוח במחשבים אישיים לגשת לספריה משותפת בשרת קבצים*

יישומי מערכת-שיתוף-קבצים גם מציבים מספר בעיות אבטחה. עם יישום מרכזי, נושאי אבטחה מוגבלים, למעשה, למערכת המחשב המארח וניתן לפתור אותם שם. אולם, כדי שיישום מערכת-שיתוף-קבצים יפעל, כל מחשבי הלקוח חייבים להיות בעלי כושר לקרוא ולכתוב נתונים אל המקום שבו נמצאים הנתונים המשותפים וממנו. בנוסף, כל מחשבי הלקוח חייבים לשתף פעולה, כדי להבטיח שקבצי הנתונים לא ייפגעו מגישה בו-זמנית של מספר משתתפים. במקרים רבים, ניתן להשיג זאת על ידי מנגנון **נעילת קובץ** (file-locking) או מנגנון **נעילת רשומה** (record-locking), המוסיפים תקורה לזמן העיבוד ויוצרים תעבורת רשת נוספת.

עם התפתחות הרשתות ותחילת המעבר ממערכות מבוססות מחשב מרכזי גדול למערכות מבוססות מחשבים אישיים, התפתחו יישומי מערכת-שיתוף-קבצים כדי לספק חלופה ליישומים מרכזיים. למרות שמקומם שמור, במיוחד במשרדים וארגונים קטנים, אנו עדים לכך שבסביבות רבות יישומי מערכת-שיתוף-קבצים מוחלפים ביישומי שרת/לקוח, כפי שהדבר קורה ביישומים מרכזיים.

יישומי שרת/לקוח

תהליך העיבוד מתבצע הן במחשב המארח והן במחשב האורח.

כאשר אתה פועל בסביבת World Wide Web) WWW), אתה נמצא בסביבת מחשוב של יישומי שרת/לקוח (client/server applications). לדוגמה, כאשר ברצונך לראות אתר ב- Web, אתה מקליד את כתובתו בתוכנת הגלישה ברשת (או בוחר אותה מרשימת סימניות, או דף Web אחר). תוכנת הגלישה ברשת שולחת את בקשתך אל שרת Web האחראי על אתר זה. שרת Web מקבל את הבקשה ושולח אליך את קובץ HTML המייצג את הדף המבוקש.

תוכנת הגלישה ברשת מקבלת את קובץ HTML, מגדירה אותו עבור המסך שלך, קובעת אם יש צורך לבקש גרפיקה נוספת ומציגה לפניך את הדף. אין קשר נוסף עם שרת Web. תוכנת הגלישה מאפשרת לך לראות את הדף בנוסף לניהול כל פעילויות המנהלה האחרות, כגון הצגת המשך הדף כאשר אתה מדפדף. כאשר אתה לוחץ על קישור להצגת דף אחר, תוכנת הגלישה ברשת שולחת בקשה לשרת Web עבור הדף המתאים, וחוזרת על תהליך ההצגה של הדף החדש.

לעיתים, העיבוד מפוצל בין תוכנת הגלישה ברשת לבין השרת. כשאתה ממלא טופס Web ולוחץ על לחצן לשליחת הטופס המוכן, תוכנת הגלישה ברשת לוקחת את כל המידע המוזן, עורכת ודוחסת אותו, ושולחת חבילת נתונים זו בשטף אל שרת Web. השרת שולף את הנתונים מתוך החבילה הדחוסה שקיבל, מסדר אותם שוב ומעביר אותם לטקסט או תוכנית. הוא שולח תגובה כלשהי לתוכנת הגלישה בצורת קובץ HTML או טקסט. תוכנת הגלישה עורכת מחדש את הקובץ ומציגה אותו למשתמש. כלומר, לפנינו שילוב בין תוכנית הגלישה במחשב הלקוח לבין תוכנית בשרת Web.

יישומי שרת/לקוח משלבים את היתרונות של יישומים מרכזיים ושל יישומי מערכת-שיתוף-קבצים. תוכניות לקוח מטפלות בכל הפעילויות שבין המשתמש לבין המערכת ובתצוגת הנתונים, בשעה שתוכניות שרת מבצעות את עיבוד הנתונים. מודל מחשוב זה גם מנצל ביעילות רבה יותר את המשאבים העומדים לרשותו. בדרך כלל, למחשבים אישיים על שולחן העבודה יש עוצמת חישוב מספיקה לטיפול בחלונות והזנת נתוני משתמש, אולם אין להם בהכרח יכולת עיבוד לביצוע פעולות חיפוש ואחזור במסדי נתונים גדולים. ניתן לצייד את השרת במשאבים מספיקים (מעבדים, זיכרון ועוד) לביצוע פעולות מקיפות במאגרי נתונים גדולים. השרת גם יכול לאפשר למשתמשים רבים לגשת בו-זמנית למקור נתונים, בין אם זהו אתר Web, מסד נתונים, או מערכת דואר אלקטרוני.

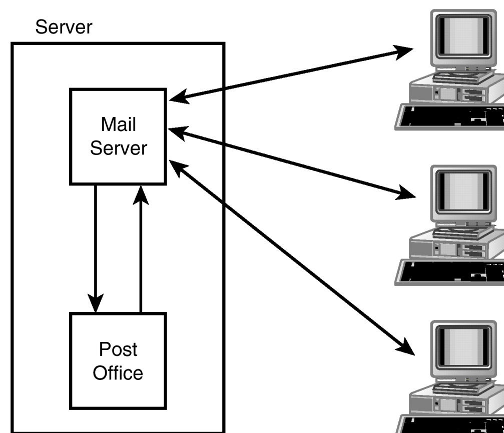


הערה: העיבוד המבוצע על ידי השרת ברקע, ולא מול עיני המשתמש, נקרא לעיתים back-end processing - עיבוד ברקע.

לדוגמה, נבחן כיצד דוגמת הדואר האלקטרוני מהסעיף הקודם תפעל בסביבת שרת/לקוח. כפי שמוצג בתרשים 10.3, תוכניות הדואר במחשבי הלקוחות פועלות כעת מול תוכנית שרת דואר. שרת הדואר, בתורו, פועל מול משרד הדואר עצמו, הנקראת **מחסן מידע** (information store) או **מחסן הודעות** (message store).

נוהל זה מציע מספר יתרונות משמעותיים על פני גישת מערכת-שיתוף-קבצים. ראשית, תוכניות דואר של לקוח אינן חייבות להיות מעורבות במבנה משרד הדואר. במקום לספק את ההודעה, הן מעבירות אותה לשרת הדואר, כדי שהוא יספק אותה.

שנית, תוכניות הדואר של הלקוח אינן חייבות להמשיך ולבדוק את מצב קובץ הדואר על השרת. שרת הדואר שם לב כאשר דואר חדש מגיע עבור המשתמש ומודיע לו שהגיעה הודעה עבורו. מכיון שתקשורת יכולה להתרחש בשני הכיוונים, **תעבורת הרשת מצטמצמת** מכיון שאין צורך בדגימה סדירה לחיפוש הודעות.



תרשים 10.3: *יישומי שרת/לקוח מחלקים את העיבוד בין מחשב הלקוח לבין מחשב השרת*

בנוסף, האבטחה טובה יותר בתרחיש זה. תוכניות דואר של לקוחות אינן ניגשות ישירות למחסן ההודעות. על כן, הן אינן זקוקות להרשאות קריאה/כתיבה לספריה זו שבשרת הקבצים, ואינן צריכות לעסוק בנעילת קבצים. שרת הדואר הוא התוכנית היחידה הניגשת למחסן ההודעות. יישומי שרת/לקוח נפוצים למדי בעולם הרשתות כיום. מעבר לשימוש ב-Web ובמערכות דואר אלקטרוני, נמצא שיישומי שרת/לקוח חוללו מהפכה באופן הגישה למסדי נתונים ברשת. על אף השימוש היעיל יותר הן ברכיבי הלקוח והן ברכיבי השרת, החיסרון העיקרי והבולט של יישומי שרת/לקוח הוא שבמקרים רבים קשה יותר לעצב ולהגדיר אותם בהשוואה ליישומי מערכת-שיתוף-קבצים, או יישומים מבוססי מארח.



רעיון מפתח

בנוהל יישומי שרת/לקוח, העיבוד מתחלק בין לקוח הפועל מול המשתמש לבין שרת המבצע פעולות ועיבוד נתונים ברקע (back-end).

דואר אלקטרוני

למרות שהשימוש הראשוני ברשתות היה אולי לשיתוף קבצים, לא עבר זמן רב עד שהמתכנתים הבינו שרשתות יכולות להוות אמצעי תקשורת מצוין ביניהם. כך החלו להופיע **יישומי דואר אלקטרוני - e-mail** (electronic mail applications) שיכלו לפעול על מערכות מסוגים שונים. כמו רוב יישומי הרשת, גם יישומי דואר אלקטרוני החלו בסביבת היישומים המרכזיים מבוססי מארח, הפועלים במחשבים גדולים והתפתחו עם הזמן ליישומי מערכת-שיתוף-קבצים וליישומי שרת/לקוח על מחשבים אישיים.

מכיון שמשלוח וקבלה של דואר אלקטרוני כרוכים בדרך כלל במספר יישומים שונים, תיתקל במקרים רבים במונחים **מערכות דואר אלקטרוני** (e-mail systems) או **מערכות הודעות** (messaging systems). רוב מערכות הדואר האלקטרוני מאפשרות למשתמשים לשלוח ולקבל הודעות מול משתמש אחד או משתמשים רבים, ו**לצרף** (attach) קבצים להודעות אלו. בדרך כלל מערכות דואר אלקטרוני מאפשרות למשתמשים גישה מרחוק להודעות שלהם. **קבלות החזר** (return receipts) ו**הודעות מסירה** (delivery notification alerts) הן תכונות נפוצות במערכות אלו.

פרוטוקולי דואר אלקטרוני

מכיון שליישומי דואר אלקטרוני יש תקני תקשורת המיוחדים להם, עליך להכיר את הפרוטוקולים שבסעיף זה. הם מגדירים את שיטת הכתובות, נהלי צירוף קבצים וכיצד הודעות מועברות בין משתמשים. יישומי דואר אלקטרוני אחדים עדיין משתמשים בפרוטוקולים קנייניים, אולם כיום רובם תומכים בפרוטוקולים פתוחים, כמו אלה הפועלים באינטרנט.

> **רעיון מפתח**
> עליך לוודא שאינך מבלבל בין פרוטוקולי התקשורת השונים לדואר אלקטרוני.

פרוטוקולי דואר אלקטרוני מתחלקים לשלושה סוגים :

- ✯ **פרוטוקולי העברה/מסירה** (Transport/Delivery),
- ✯ **שירותי ספריה** (Directory services),
- ✯ **ממשקי תכנות יישומים להודעות** (Messaging Application Programming Interfaces).

פרוטוקולי העברה/מסירה

פרוטוקולי העברה/מסירה (Transport/Delivery) אחדים עוסקים בפעולות העברה ומסירה של דואר אלקטרוני. אלה כוללים את :

- ✯ **SMTP** - Simple Mail Transport Protocol משמש לתקשורת בין שרתי דואר אלקטרוני באינטרנט. הוא מתאר כיצד שרתי דואר אלקטרוני צריכים לשלוח ולקבל הודעות. סגנון הכתובות באינטרנט (user@domain) מקורו בפרוטוקול זה.
- ✯ **POP3** ו- **IMAP4**. הבעיה עם SMTP היא שמחשבים צריכים להיות מקוונים (on-line) כל העת לשימוש בו. אם המחשב אינו מקוון, הודעות עלולות להידחות. בדרך כלל שרתי דואר אלקטרוני מקוונים, ולכן העברת הודעות בפרוטוקול SMTP פועלת היטב. אולם מכיון שרוב המחשבים האישיים אינם מחוברים כל העת לאינטרנט, פותח מנגנון אחר להעברת הודעות. SMTP משמש למסירת הודעה לתיבת הדואר שלך בשרת דואר אלקטרוני, אך כאשר אתה מחייג בעזרת המחשב האישי אל השרת, אתה מקבל ממנו את ההודעות באמצעות

Post Office Protocol version 3 (POP3). למרות ש-POP3 מספיק לצורך זה, הוא נמצא בתהליכי שדרוג לתוכנה חדשה - Internet Mail Access Protocol version 4 (IMAP4).

- **MIME**. תקן Multipurpose Internet Mail Extension מגדיר את הדרך שבה קבצים מצורפים להודעות SMTP.
- **X.400**. תקני X.400 של International Telecommunication Union מגדירים מגוון פרוטוקולים להעברת דואר בין שרתי דואר אלקטרוני. תקני X.400 עוסקים בכתובות לממשקי משתמש, בממשקי משתמש, בפרוטוקולי העברה ובהוראות מסירה. X.400 משמש במקרים רבים באפיקי שידרה בין שרתי דואר אלקטרוני בארגונים.
- **MHS**. Message Handling Service של נובל הוא התקן המקובל להעברת דואר אלקטרוני בסביבות Novell NetWare. הוא דומה ל-SMTP ו- X.400 בכך שהוא פועל ברקע במהלך העברת הודעות.

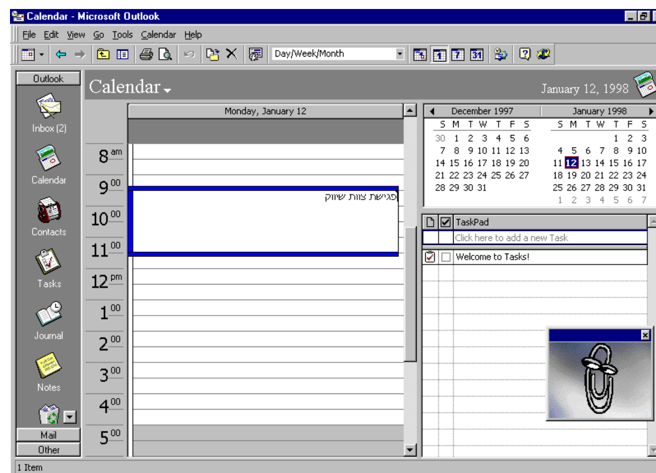
חיבור מערכות דואר אלקטרוני

מכיון שמרבית מערכות הדואר האלקטרוני (e-mail) מיועדות לאפשר מספר גדול של משתמשים, מערכת דואר אלקטרוני יחידה עשויה לענות במידה רבה על צרכי הארגון שלך. אולם, בנקודה כלשהי תיתקל בצורך לתקשר עם מערכות דואר אלקטרוני אחרות. ייתכן שכתוצאה ממיזוג יהיה עליך לשלב שתי מערכות שונות, או שהמשתמשים דורשים יכולת לשלוח דואר אלקטרוני למשתמשי אינטרנט. בכל מקרה, רוב מערכות הדואר האלקטרוני כיום יכולות להחליף הודעות עם מערכות אחרות.

מערכות הודעות אחדות, כמו Microsoft Exchange, כבר מגיעות עם מספר קשרים המאפשרים חיבור קל למערכות אחרות. מערכות אחרות, כמו Microsoft Mail, דורשות בדרך כלל רכישה והתקנה של תוכנית **שער** (gateway) נפרדת. תוכנת השער לעיתים יכולה לפעול על מחשב קיים, אולם עשויה להזדקק למחשב ייעודי נפרד. חברות רבות כיום משתמשות באינטרנט כדרך לחבר מספר מערכות.

תזמון (Scheduling)

יישומי תזמון למשתמש, ידועים במחשבים האישיים מזה שנים רבות. בדרך כלל יישומים מסוג זה מאפשרים לראות את לוח הזמנים שלך עבור היום, השבוע, החודש, או השנה הקרובים, ומאפשרים לבצע שינויים מהירים בלוח זמנים זה. ניתן לקבוע זמנים לאירועים על פני מספר ימים ובשעות שונות. בדרך כלל ניתן לקבוע **מתריעים** (alerts) שיודיעו בדרך כלשהי לפני תחילת פגישה צפויה. אם תנסה לקבוע פגישה בשעה שכבר מתוכנן משהו, תוכנת התזמון יכולה להתריע על הסתירה ולאפשר לך לפתור אותה. Microsoft Outlook, המוצג בתרשים 10.4, הוא דוגמה לתוכנה המשלבת אפשרות תזמון. דוגמאות אחרות הן : +Microsoft Schedule ו- Lotus Organizer.



תרשים 10.4: *Microsoft Outlook מספקת יכולות תזמון לקבוצה או ליחיד*

יישומי תזמון ברשת יכולים להיות יתרון גדול לארגונים ולאפשר למשתמשים לתזמן ביעילות רבה יותר פגישות של העובדים. עם זאת חשוב להדגיש שכדי להשיג זאת, כל חברי הקבוצה, או העובדים בחברה, חייבים **להשתמש** בפועל ביישום התזמון ולתחזק את לוחות הפגישות כראוי!

קובצה (Groupware)

יישומי קובצה (Groupware), הנקראים גם יישומי קבוצת עבודה (workgroup applications), דומים למערכות דואר אלקטרוני. אולם, יישומי קובצה מספקים שירותים נוספים המיועדים לאפשר לקבוצת אנשים לפעול טוב יותר יחד. מערכות קובצה אחדות, כגון Microsoft Exchange, GroupWise ו- Lotus Notes, מספקות הן פעולות דואר אלקטרוני והן פעולות קובצה. מוצרי קובצה אחרים עשויים להתמקד בהיבט מסוים יחיד בעבודה המשותפת כמו Work Flow, ניהול יומנים,

מסדי נתונים משותפים

מבראשית, רשתות מחשבים סיפקו למשתמשים גישה למערכות מסדי נתונים גדולות. **מערכות ניהול מסדי נתונים - DBMS** (Database Management Systems) מרכזיות, ואחר כך מערכות שרת/לקוח, פותחו לשיתוף מידע ברשת. למרות שבעבר יישומים מרכזיים היו הנורמה, כיום רוב הרשתות משתמשות בסוג כלשהו של יישום שרת/לקוח. **מנוע DBMS** (DBMS engine) פועל בשרת ומספק גישה מהירה לנתוני הארגון. יישומי לקוח על מחשבים אישיים שולחים **שאילתות** (queries) אל מנוע ניהול מסד הנתונים. תעבורת הרשת כוללת את השאילתות מהלקוח ואת קבוצות הנתונים הנשלחים חזרה מהשרת. דוגמאות DBMS ברשתות מיקרוסופט אופייניות כוללות את Microsoft SQL server ו- Microsoft Access.

כמו ביישומי דואר אלקטרוני, גם ליישומי DBMS יש מספר תקנים שונים. אולם קהילת ספקי תוכנות DBMS גיבשה שני תקנים עיקריים בלבד והסכימה עליהם:

- **SQL** - Structured Query Language (שפת שאילתות מובנית) היא **שפת גישה לנתונים** (data access language) המשמשת כמעט בכל יישומי מסד נתונים מסוג שרת/לקוח. השאילתות הנשלחות על ידי הלקוח לשרת מורכבות ממשפטי SQL.
- **ODBC** - Open Database Connectivity (קישור מערכות פתוחות) של מיקרוסופט היא ממשק תכנות יישומים המאפשר למפתחי יישומי Windows לשלב קישורים למסדי נתונים בתוך היישומים שלהם. בדיוק כפי שדרייברים לכרטיסי ממשק רשת (NIC) מאפשרים למחשב לתקשר עם כל NIC, כך דרייברים של ODBC מאפשרים ליישום לתקשר עם כל מסד נתונים. כאשר יישום רוצה להגיש שאילתה, דרייבר ODBC ממיר את השאילתה לאוסף משפטי SQL (פקודות), ושולח אותם אל מנוע מסד הנתונים המתאים.

כפי שהסברנו קודם, בדיון אודות יישומי מערכת-שיתוף-קבצים בפרק זה, ניתן להפעיל יישום מסד נתונים בגישת מערכת-שיתוף-קבצים. יישומי מסד נתונים זולים רבים נוקטים בגישה זו, שיכולה להתאים לסביבת עבודה קטנה. אולם על פי מודל זה, יישומי מסד נתונים צורכים רוחב פס גדול ברשת. בדרך כלל יש להעתיק את כל מסד הנתונים משרת הקבצים אל מחשב הלקוח בו הוא מעובד, ולאחר מכך הוא נשלח חזרה אל שרת הקבצים. עם גידול הרשת, תעבורת רשת גדולה עלולה לגרום לכך שיישום שרת/לקוח יהיה בחירה אטרקטיבית הרבה יותר.

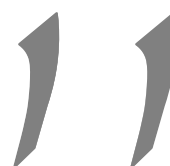
סיכום

יישומי רשת, הפועלים בשכבת היישום (application) של מודל ייחוס OSI, מספקים את הפונקציונליות הגורמת לרשתות להיות שימושיות.

יישומים יכולים לתפקד במספר רמות ברשת. יישומים עצמאיים מסורתיים יכולים לשמור ולאחזר קבצים באמצעות שרתי קבצים. גרסאות רשת של יישומים עצמאיים יכולים להיות מוצבים על שרת קבצים ולספק למנהלי הרשת אמצעי נוח לניהול היישום.

בנוסף, קיימים יישומים שתוכננו במיוחד לשימוש בסביבה מרושתת, כולל דואר אלקטרוני, תזמון, קובצה ומסדי נתונים משותפים.

יישומי רשת אמיתיים יכולים להשתמש בשלושה מודלי מחשוב שונים. יישומים מרכזיים מרכזים את כל עוצמת החישוב במחשב המארח והלקוח מספק רק חלון עבודה למחשב זה. יישומי מערכת-שיתוף-קבצים, לעומת זאת, מבצעים את כל העיבוד במחשב הלקוח ומשתמשים בשרת לאחסון קבצי נתונים בלבד. יישומי שרת/לקוח מפצלים את העיבוד בין מחשב הלקוח לבין מחשב השרת. הלקוח מטפל באינטראקציה עם המשתמש, והשרת מבצע את הפעולות על הנתונים. יישומי שרת/לקוח מייעלים את השימוש במשאבי רשת ובעוצמת החישוב שנמצאת במחשב האישי על שולחן העבודה, ומהווים את המודל השולט ביישומי רשת חדשים.



גישה מרחוק

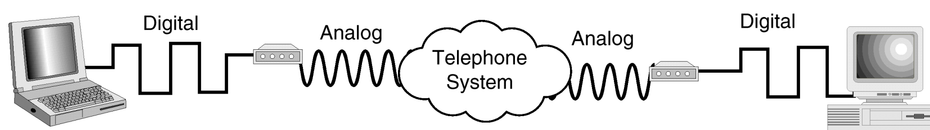
ככל שרשתות מתחילות למלא תפקיד גדול יותר בארגון, תיווכח שמשתמשים ירצו בקרוב יכולת גישה לרשת ממקומות מרוחקים. פרק זה ידון במה שצריך לעשות כדי לספק שירות זה מהרשת. כשתגיע לסיום הלימוד בפרק זה, תוכל:

- להסביר כיצד פועלים מודמים,
- לתאר את סוגי המודמים השונים,
- לתאר את תוכנת הגישה מרחוק המשמשת במערכות הפעלה של מיקרוסופט,
- לזהות את התנאים המתאימים לשימוש בפרוטוקולי SLIP ו-PPP.

מודמים

לאורך זמן, ככל שרשתות יהפכו קריטיות לפעילויות של הארגון, ירצו משתמשים לגשת למשאבי הרשת הארגונית כאשר הם נמצאים מחוץ למשרד המרכזי. בין אם הם בבית, במשרד מרוחק, אצל לקוח, או בחדר במלון בעת מסע עסקים, הם ירצו להתחבר אל הרשת המשרדית שלהם. התשובה הפשוטה ביותר היא לאפשר למשתמשים אלה להתקשר לרשת המשרדית באמצעות קו טלפון. אך, מכיון שמחשבים משתמשים באותות דיגיטליים (סיביות) וקווי טלפון משתמשים באותות אנלוגיים (קול), אין דרך לחבר את המחשב לקו הטלפון סתם כך.

כדי להשיג את המטרה של תקשורת על פני קו טלפון, עליך להשתמש ב**מודם** (modem). כפי שמוצג בתרשים 11.1, המשימה העיקרית של מודם היא להמיר סיביות "1" ו-"0" של אות דיגיטלי לגל קול אנלוגי שישודר על פני קו הטלפון. בקצה המקבל, מודם נוסף ממיר את האות האנלוגי בחזרה לאות דיגיטלי.



תרשים 11.1: *מודם ממיר את האות הדיגיטלי של המחשב לאות אנלוגי שיועבר בקו טלפון*



רעיון מפתח

מודם הוא התקן **שמאפנן** (MOdulate) אות נתונים דיגיטלי לאות אנלוגי **ומפענח** (DEModulate) אות אנלוגי לאות דיגיטלי (מחזיר אותו לאות "קריא במחשב").

מודמים זמינים בדרך כלל לחיבור פנימי או חיצוני למחשב. מודם פנימי מתחבר לחריץ הרחבה בלוח האם של המחשב, ומספק שקע RJ-11 (שקע טלפוני לארבעה חוטים), שממנו ניתן לחבר כבל טלפון רגיל בין המודם לתקע הטלפון.

מודם חיצוני הוא קופסה נפרדת המחוברת למחשב באמצעות כבל טורי (המוכר ככבל RS-232). למודמים חיצוניים יש שקע RJ-11 לחיבור לטלפון, ובדרך כלל יש להם נוריות לחיווי מצבים שונים של המודם.

מהירות המודם נמדדת במספר סיביות לשנייה - bps (סל"ש) שהוא יכול להעביר בקו הטלפון, או לקבל מקו הטלפון. כפי שמוצג בטבלה 11.1, איגוד התקשורת הבינלאומי (ITU) פיתח תקנים בשם V-series להגדרת מהירויות מודם. שים לב שחלק מסימוני התקנים כוללים את המילה bis ו-terbo. סימונים אלה אינם קשורים למהירות, אלא למילה הצרפתית "שנייה" או "שלישית", ומציינים שאלו הן גרסאות של תקנים מתקדמים יותר.

טבלה 11.1: *תקני ITU למודמים*

תקן	bps
V.22bis	2,400
V.32	9,600
V.32bis	14,400
V.32terdo	19,200
V.3FastClass (V.FC)	28,800
V.34	28,800
V.35, V.42bis, V.90	57,600

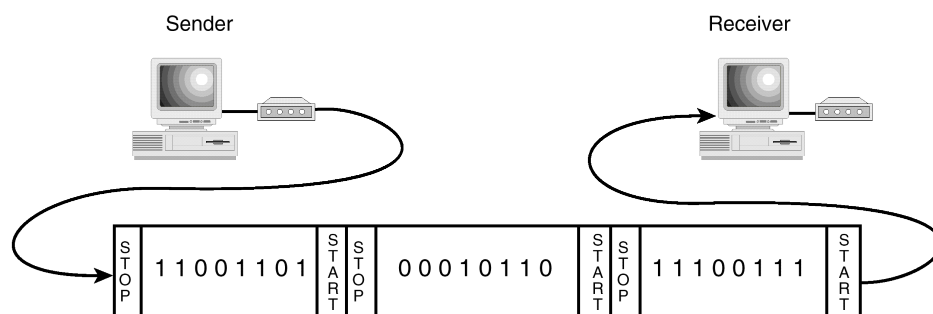
כיום מקובלים בשימוש שני סוגי מודמים:

- ✯ **אסינכרוניים** (Asynchronous)
- ✯ **סינכרוניים** (Synchronous)

סוג המודם שבו תשתמש יהיה תלוי בסוג קו הטלפון שתשתמש בו.

מודמים אסינכרוניים (Asynchronous)

מודמים אסינכרוניים (או async) נמצאים בשימוש נרחב ברוב רשתות התקשורת. הם מיועדים לשימוש עם קו טלפון רגיל, וכן הם ממירים כל בית (byte) של נתונים לזרם של סיביות "1" ו-"0". כפי שמוצג בתרשים 11.2, כל בית ארוז בין סיבית התחלה (start bit) לסיבית סיום (stop bit).



תרשים 11.2: *מודמים אסינכרוניים אורזים נתונים בין סיביות התחלה וסיום*

לפני תחילת התקשורת, המודם השולח והמודם המקבל חייבים להסכים ביניהם על מהירות השידור וסדר סיביות ההתחלה והסיום. רק אז התקשורת תצליח.

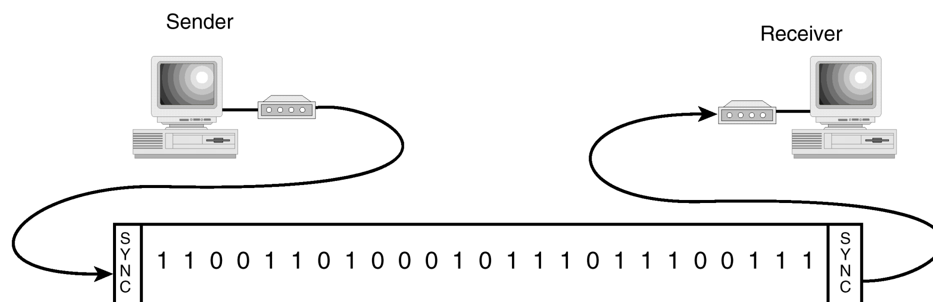
בנוסף לסיביות התחלה וסיום, מודמים רבים משלבים סוג כלשהו של בדיקת שגיאות, כדי להבטיח שהנתונים מועברים כהלכה בקו הטלפון. השיטה הפשוטה ביותר לבדיקת שגיאות כרוכה בסיבית **זוגיות** (parity) אשר נוספת לשידור של כל בית. באופן עקרוני, בדיקת זוגיות פועלת כך: המודם השולח סופר כמה סיביות "1" יש בזרם הנתונים עבור כל בית. אם המספר אי-זוגי, סיבית הזוגיות נקבעת ל-1. בקצה השני, המודם המקבל סופר גם הוא את מספר הסיביות "1" וקובע אם המספר זוגי או אי-זוגי. המודם המקבל משווה את התוצאה שלו, עם סיבית הזוגיות שקיבל ("1" או "0"). אם התוצאה תואמת, קרוב לוודאי הנתונים נכונים, ומועברים לעיבוד. אם אין התאמה, המודם המקבל מבקש שידור חוזר של מנת נתונים זו (packet) וימשיך לבקש עד לקבלה תקינה של מנת הנתונים כולה.

רוב המודמים האסינכרוניים משלבים סוג כלשהו של דחיסת נתונים להשגת מהירויות העברה גבוהות יותר. אחד מפרוטוקולי הדחיסה הנפוצים הוא V.42bis.

בעוד שכל בדיקות השגיאות והדחיסה מאפשרות תקשורת אמינה, אמינות זו מושגת במחיר. מודמים אסינכרוניים רבים משתמשים בכמעט 25 אחוזים של משאבי השידור לבדיקת שגיאות ולבקרה.

מודמים סינכרוניים (Synchronous)

מודמים אסינכרוניים תלויים בסיביות התחלה וסיום כדי לקבוע היכן נתונים מתחילים ומסתיימים, ולעומתם מודמים סינכרוניים תלויים בתזמון. שני המודמים צריכים להיות מתואמים ביניהם (מסונכרנים בזמן), כדי שהתקשורת תצליח. כפי שמוצג בתרשים 11.3, מודמים סינכרוניים משדרים נתונים במסגרות, ומדי פעם הם משלבים בין הנתונים סיבית סנכרון (sync) להבטחת דיוק התזמון.



תרשים 11.3: *מודמים סינכרוניים תלויים בתזמון מדויק לשידור נתונים ומשתמשים בסיביות סנכרון כדי להבטיח שהנתונים מועברים בצורה מדויקת*

מכיון שמודמים סינכרוניים אינם זקוקים לסיביות ההתחלה והסיום המשמשות מודמים אסינכרוניים, הם יכולים להגיע לקצבי העברת נתונים גבוהים הרבה יותר מאשר מודמים אסינכרוניים. אולם, מכיון שמודמים סינכרוניים אינם מיועדים לשימוש בקווי טלפון רגילים, נמצא אותם בעיקר בקווים ייעודיים חכורים. מודמים סינכרוניים יכולים גם לשמש לחיבור מרחוק למחשבים גדולים של יבמ (mainframe).

מודמים דיגיטליים

למעשה, **מודמים דיגיטליים** אינם ממש מודמים, אלא פיתוח מחלקות השיווק של יצרני ציוד תקשורת לרשתות ISDN (Integrated Services Digital Network). רשת מסוג ISDN, שתתואר בהמשך פרק זה, ובפירוט רב יותר בפרק 13 העוסק ב"רשתות מרחביות (WANs)", מספקת חיבור דיגיטלי לחלוטין במהירויות של עד 128Kbps (כלומר, 128,000bps). התקן החיבור של ISDN מורכב מהתקן Network Termination (NT) וציוד Terminal adapter (TA). כיום, שני הרכיבים ארוזים בקופסה אחת ונקראים בכל אחד מהשמות.

מתוך הכרה שמשתמשים במחשבים מכירים מודמים רגילים, יצרני ISDN החלו לקרוא להתקן NT/TA בשם **מודם דיגיטלי**, בניסיון למשוך אנשים לשימוש ברשתות מסוג ISDN. "מודמים" דיגיטליים יכולים לשמש **רק** עם ISDN ואינם מתאימים לקווי טלפון רגילים.



הערה: בדיוק כפי שמודמים דיגיטליים יכולים לשמש רק בקווי טלפון דיגיטליים, כמו אלה של ISDN, מודמים יכולים לפעול רק עם קווי טלפון אנלוגיים רגילים. משתמשים רבים גרמו נזק (הרסו!) את המודם במחשב הנייד שלהם, על ידי חיבור שלא בכוונה לקו טלפון דיגיטלי!

סוגי חיבורים

חשוב להכיר ולהבין את סוג המודם שהמשתמשים שלך ישתמשו בו, אך עליך גם להתייחס לסוג החיבור שישמש אותם לחיבור לרשת. בעולם PSTN (Public Switched Telephone Network), כפי שרשת הטלפונים הציבורית מכונה באופן רשמי, קיימות שלוש אפשרויות:

- חיבור בחיוג (dial-up),
- ISDN (Integrated Services Digital Network),
- קווים ייעודיים חכורים (leased lines).



הערה: PSTN, קווים ייעודיים חכורים ו-ISDN יידונו בפירוט רב יותר בפרק העוסק ב"רשתות מרחביות (WANs)".

חיבור בחיוג (dial-up connection) משתמש בקווי הטלפון הרגילים ומספק חיבור זמני בין שני אתרים. מכיון שאיכות ואמינות קווי טלפון אינה קבועה, מהירויות התקשורת מוגבלות בדרך כלל ל-28,800bps. טכנולוגית דחיסה חדשה מאפשרת להעלות את קצב השידור עד ל-56Kbps. מהירויות שידור 115Kbps הודגמו בניסויים, אולם טכנולוגיה זו אינה מופעלת באופן נרחב.



הערה: בשפת הטלקומוניקציה ייתכן ותשמע את המונח POTS (Plain Old Telephone Service) בעת התייחסות לשירות הטלפון הבסיסי.

ISDN מספק אמצעי חיוג להעברת קול ונתונים על פני קו טלפון דיגיטלי. Basic Rate ISDN מספק שני ערוצי-B בקצב 64Kbps עבור קול או נתונים, וערוץ-D אחד להקמת שיחה ובקרה. Primary Rate ISDN מספק 23 ערוצי-B וערוץ-D אחד ומשמש בעיקר לחיבורי WAN. למרות הדרישה להתקנת קו טלפון דיגיטלי מיוחד, ISDN יכול להיות מועיל מאוד לגישה מרחוק, מכיון שמשתמש BRI יכול לשלב יחד שני ערוצי 64Kbps למהירות כוללת של 128Kbps. ארגונים רבים מגלים ש-ISDN הוא אמצעי כדאי מבחינה כלכלית לחיבור אתרים מרוחקים, כאשר נדרשים רק חיבורים זמניים מדי פעם.

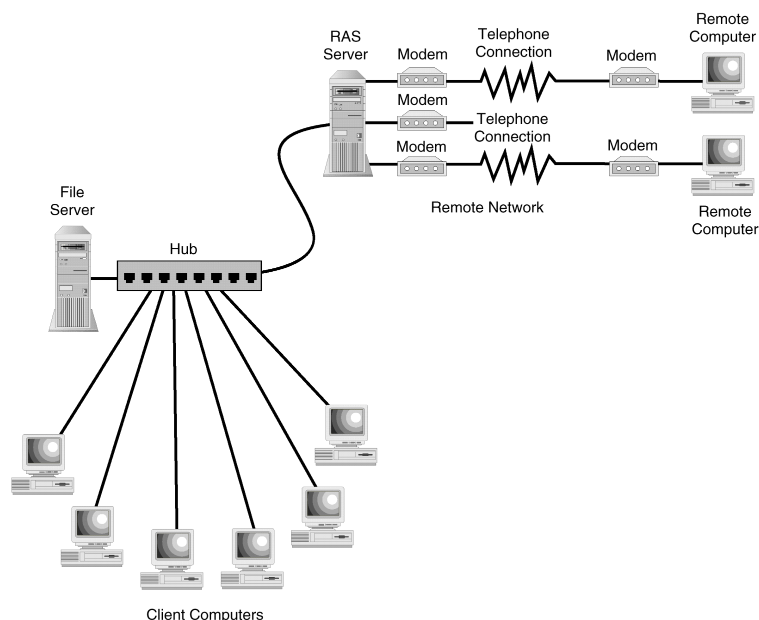
קווים ייעודיים חכורים (dedicated leased lines) כרוכים בחכירה קבועה של קו טלפון בין שתי נקודות. ניתן לחכור קווים אנלוגיים ייעודיים לשימוש עם מודמים, אולם משיקולי עלות קיימות טכנולוגיות טובות יותר ליצירת חיבורים ייעודיים בין משרדים. מידע נוסף אודות חיבורים ייעודיים תמצא בפרק 13, "רשתות מרחביות (WANs)".

תוכנת גישה מרחוק

כאשר המשתמשים מתחברים לרשת באמצעות מודם, צריכה להיות תוכנה כלשהי המאפשרת להם גישה למשאבי הרשת. ברשתות מיקרוסופט, התוכנה המטפלת בחיבורים נכנסים היא בדרך כלל Remote Access Service (RAS) המסופקת עם Windows NT. בשעה שתוכנת RAS המסופקת עם Windows NT Workstation יכולה לטפל רק בחיבור נכנס יחיד, RAS ב- Windows NT Server יכולה לנהל עד 256 חיבורים נכנסים. כפי שמוצג בתרשים 11.4, תרחיש אופייני הוא הקצאה של שרת אחד לשימוש RAS וחיבור מספר מודמים אליו.

לאחר החיבור, יכולים המשתמשים לגשת למשאבי הרשת כאילו היו מחוברים אליה ישירות. יהיה כמובן הבדל במהירות כתוצאה מכך שמודמים יכולים לפעול במהירות מסדר גודל של 28.8Kbps ואילו רשתות פועלות ב-10Mbps. כמובן שבעיה זו פחותה עבור משתמשי ISDN המתחברים ב-128Kbps, אולם גם במקרה זה הביצועים לא יהיו מהירים כמו בחיבורי LAN ישירים.

תוכנת שרת RAS קלה להגדרה. לאחר חיבור מודם לכניסה מסוימת, יש להגדיר לתוכנת שרת RAS לקבל שיחות נכנסות לכניסה זו ולהפעיל את שירות Windows NT RAS.



תרשים 11.4: *שרת המריץ RAS יכול לספק גישה מרחוק לרשת מיקרוסופט*



רעיון מפתח

שרת RAS הוא מחשב Windows NT/2000 המוגדר להשתמש בתוכנת RAS Server כדי אפשר למשתמשים רחוקים להתחבר לרשת באמצעות מודמים.

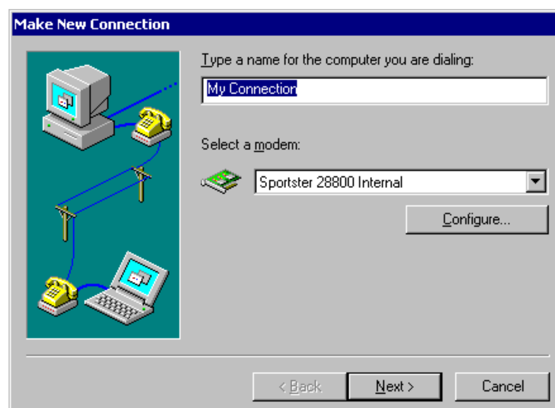
ב-Windows 95 וב-Windows NT 4.0, תוכנת הלקוח המרוחק נקראת Dial-Up Networking ובקיצור **DUN**. DUN מספקת ממשק קל לשימוש ב- Windows, הדומה לממשק לקוח RAS הכלול ב- Windows NT/2000, תרשים 11.5 .

הן לקוחות RAS והן לקוחות DUN יכולים להתחבר אל מחשב Windows NT המריץ תוכנת שרת RAS. בנוסף, ניתן להשתמש בתוכניות לחיבור ישיר אל ספקי שירותי אינטרנט לצורך גישה לאינטרנט.



רעיון מפתח

מערכות הפעלה של מיקרוסופט מספקות לקוח RAS (Remote Access Service) או לקוח DUN (Dial-Up Networking) המאפשרים למשתמשים להתחבר למערכות מרוחקות.



תרשים 11.5: *Dial-Up Networking ב- Windows 95 כוללת אשף Add New Connection המקל על יצירת חיבורים חדשים*

פרוטוקולי תקשורת מרחוק באמצעות קו טלפון

בעת שימוש בלקוח RAS/DUN המתואר לעיל, תוכל לבחור בפרוטוקול התקשורת לחיבור. לקוח RAS/DUN יכול לתמוך בשני פרוטוקולי תקשורת:

- ✯ Serial Line Internet Protocol (**SLIP**) - פרוטוקול קו טורי לאינטרנט,
- ✯ Point to Point Protocol (**PPP**) - פרוטוקול נקודה לנקודה.

ניתן להגדיר את הפרוטוקול בלקוח באמצעות תיבת דו-שיח מתאימה בלקוח RAS/DUN.

Serial Line Internet Protocol (SLIP)

פרוטוקול זה מתפקד בשכבה הפיסית של מודל ייחוס OSI. כאשר עובדים עם פרוטוקול זה יש להגדיר IP Address בצורה ידנית. זוהי הסיבה שספקיות האינטרנט (ISP) לא עובדות איתו.

Serial Line Internet Protocol (SLIP) - פרוטוקול קו טורי לאינטרנט - הוא פרוטוקול ישן שפותח בעיקר כדי לאפשר למחשבים אישיים להתחבר לאינטרנט באמצעות מודם. הוא מספק תפקודי שכבה פיסית של מודל ייחוס OSI בכך שהוא מאפשר לנתונים לזרום בקו הטלפון אל מערכת מרוחקת. SLIP אינו מספק בדיקת שגיאות וסומך על החומרה שתבצע זאת. SLIP תומך בחיבור לרשתות TCP/IP בלבד, ואינו זקוק לכתובות מכיון שהחיבור מבוצע רק בין שני מחשבים. SLIP אינו מספק דחיסת נתונים, אולם קיימת גירסה הנקראת Compressed SLIP (CSLIP) המציעה דחיסה.



רעיון מפתח

Serial Line Internet Protocol (SLIP) תומך בפרוטוקול רשת אחד בלבד, TCP/IP, ואינו מספק בדיקת שגיאות או דחיסה.

Point to Point Protocol (PPP)

פרוטוקול זה מתפקד בשכבה הפיסית ובשכבת הקישור של מודל ייחוס OSI.

Point to Point Protocol (PPP) - פרוטוקול נקודה לנקודה - מספק חיבור הרבה יותר טוב ואמין בין מחשבים. ההבדל הגדול ביותר ביחס ל-SLIP הוא בכך ש-PPP מספק תפקוד הן בשכבה הפיסית והן בשכבת קישור הנתונים של מודל ייחוס OSI. למעשה, הוא הופך את המודם לכרטיס ממשק רשת. באמצעות תפקודים נוספים אלה, PPP תומך במספר פרוטוקולי רשת כגון IP, IPX, ו-NetBEUI. בנוסף, PPP מספק דחיסה ובדיקת שגיאות ההופכים אותו למהיר ואמין יותר מאשר SLIP.

בשכבת קישור הנתונים, PPP אורז נתונים למסגרות ומספק מנגנוני בדיקת שגיאות כדי להבטיח העברה מדויקת של נתונים. PPP גם משלב את הפרוטוקול Link Control Protocol (LCP) - פרוטוקול בקרת קישור - המקים את בקרת הקשר הלוגי בין שני המחשבים שמתקשרים זה עם זה.

למרות שגם SLIP וגם PPP משמשים לחיבור לרשתות TCP/IP, אנו רואים ש-PPP מציע את היתרון הנוסף לתמיכה בהקצאת כתובות IP דינמית. התמיכה בכתובות דינמיות מאפשרת למנהלי רשת להקצות תחום כתובות עבור מודמים של RAS ולאפשר למשתמשים להשתמש רק בכתובות אלו.

למרות ש-SLIP היה הפרוטוקול העיקרי ששימש מחשבים אישיים לחיבור לאינטרנט, PPP מחליף אותו כעת כפרוטוקול הבחירה לחיבורי TCP/IP.



רעיון מפתח

PPP מספק תקשורת מרחוק, מהירה ואמינה, על פני מספר פרוטוקולי רשת. שלא כמו SLIP, כולל פרוטוקול PPP יכולת לתיקון שגיאות ולדחיסת נתונים.

בחירת פרוטוקול לתקשורת מרחוק

הבחירה באיזה פרוטוקול להשתמש יכולה להיות פשוטה. אם אתה מתחבר לשרת RAS הפועל על מחשב Windows NT, הברירה היחידה היא PPP. פרוטוקול SLIP מסופק במערכות הפעלה של מיקרוסופט רק עבור חיבורי **לקוח RAS**.



רעיון מפתח

שרת RAS של Windows NT תומך בחיבורי PPP בלבד, אך לא בחיבורי SLIP.

למעשה בעת חיבור למערכות אחרות, הבחירה תלויה בכישורי המערכת המרוחקת שאליה אתה מתחבר. מכיון ש-PPP מהיר ואמין יותר מ-SLIP, הוא יהיה תמיד האפשרות המועדפת. למרות שתמצא שימוש מוגבל ב-SLIP, במיוחד בסביבות UNIX, תיווכח שמרבית הרשתות המרוחקות משתמשות כיום ב-PPP.



הערה: מרבית ספקי שירותי אינטרנט מספקים חיבורי PPP בלבד.



רעיון מפתח

אל תבלבל בין PPP לבין PPTP. לידיעתך, Point-to-Point Tunneling Protocol (PPTP) **הוא הרחבה של פרוטוקול PPP הנתמך ב-** Windows NT/2000 **ומאפשר הקמת קשר מאובטח בין שני מקטעי רשת על פני רשת** TCP/IP **כגון האינטרנט. אין זה PPP.**

אבטחת חיבורים מרחוק

כאשר אתה מאפשר חיבור מרחוק אל הרשת שלך, אתה פותח פתח שדרכו יכול פולש כלשהו לחדור אליה. בעת השימוש בתוכנת RAS (Remote Access Service) - שירותי גישה מרחוק - של מיקרוסופט, עומדות בפניך מספר אפשרויות:

- ✯ **Passwords (סיסמאות)**. כאשר משתמשים מחייגים לשרת RAS, תוכנת השרת משתמשת באבטחת Windows NT מלאה לאימות המשתמש. אם השרת הוא חלק מ**תחום** (domain) Windows NT, השם וסיסמת המשתמש יישלחו לבקר התחום לאימות. אם השרת הוא תחנת עבודה עצמאית או חלק מקבוצת עבודה, מסד הנתונים המקומי לאבטחה ישמש לאימות המשתמש.
- ✯ **Granting Dial-In Permission (הקצאת הרשאות חיוג)**. עוד לפני אימות הסיסמה, ניתן להגדיר לתוכנת שרת RAS למנוע ממשתמשים את יכולת החיבור לשרת RAS. ניתן להגדיר לכל משתמש בנפרד את יכולת החיוג אל הרשת.
- ✯ **Callback capability (יכולת חיוג חוזר).** כאשר משתמש מתחבר לשרת RAS, ניתן להגדיר את השרת כך שינתק את המודם ויתקשר חזרה אל המשתמש ליצירת החיבור. ניתן להגדיר תכונה זו למספר טלפון שייקבע מראש. כך תוכל לאפשר למשתמש להתחבר לרשת רק מהבית, או ממשרד מרוחק מוכר.

✯ **Encryption (הצפנה)**. לקוחות RAS/DUN ושרתי RAS מוגדרים אוטומטית להצפנת התקשורת בקווי טלפון בין הלקוח לשרת. ניתן להגדיר ללקוח RAS להתקשר לשרת רק ברמות הצפנה מסוימות. אם לא ניתן ליצור חיבור מוצפן, לקוח RAS יסיים את ניסיון ההתקשרות. שים לב שאם נעשה שימוש באימות ברירת המחדל כדי לאפשר התרחשות אימות כלשהו, סיסמה יכולה להישלח בטקסט רגיל (קריא) ואם גורם זר יקבל אותה, הוא יוכל לקרוא את הסיסמה.

אפשרויות אבטחה אלו לבד אינן מבטיחות שזרים לא יחדרו לרשת שלך, אולם הן בהחלט עשויות להפחית את האיום הזה.

סיכום

בעת אספקת גישה מרחוק לרשת שלך, המנגנון העיקרי שמשתמשים בו הוא חיבור בחיוג באמצעות **מודם**. מודמים הם התקנים המחוברים למחשבים המתרגמים בין האות הדיגיטלי של המחשב לאות האנלוגי (קול) של קו הטלפון. בעת שידור הנתונים, המודם ממיר את הנתונים לגלי קול אנלוגיים. בקצה המקבל, המודם ממיר את גלי הקול האנלוגיים שוב לנתונים דיגיטליים שהמחשב יכול לעבד.

קיימים שני סוגים עיקריים של מודמים: אסינכרוני וסינכרוני. בדרך כלל משתמשים **במודמים אסינכרוניים** במחשבים אישיים, המספקים חיבורים על פני קווי טלפון רגילים. מודמים אסינכרוניים משתמשים בסיביות התחלה וסיום לזיהוי ההתחלה והסוף של רצף הנתונים המשודרים ותומכים בתיקון שגיאות ודחיסה. **מודמים סינכרוניים** אינם משתמשים בסיביות התחלה וסיום, אלא מסתמכים על תיאום זמנים מדויק (סינכרון) בין המחשב השולח לבין המחשב המקבל. יש למודמים אלה תקורה נמוכה יותר מזו של מודמים אסינכרוניים, ולכן הם עשויים להגיע למהירויות שידור גבוהות יותר, אולם הם מוגבלים בעיקר לקווים חכורים ייעודיים.

כדי להתקשר אל רשת תקשורת רחוקה דרוש **קו חיבור**. משתמשים יכולים לבחור בין שימוש בקווי טלפון רגילים, קווי ISDN, או קווים חכורים ייעודיים. שימוש בקווי טלפון רגילים הוא השיטה הנפוצה ביותר לחיבור מרחוק. קווי ISDN נעשים נפוצים יותר בגלל קצב השידור הגבוה יותר שהם מאפשרים.

חיבור המודם לבדו לא יועיל ללא **תוכנה** מתאימה בשני קצות החיבור. מערכות הפעלה של מיקרוסופט כוללות את רכיב RAS (Remote Access Service) לחיבור מרחוק. תוכנת שרת RAS פועלת על Windows NT Server. תוכנת הלקוח מגיעה בצורת לקוח RAS במערכות Windows NT/2000 Sever או בצורת לקוח DUN (Dial-Up Networking) במערכות Windows 9x/ME. הן לקוחות RAS והן לקוחות DUN מאפשרים למחשבים להתחבר לשרתי RAS או ישירות אל ספקי שירותי אינטרנט (ISP).

מרכיב הגדרה נוסף הוא **פרוטוקול התקשורת** שבו ישתמש הלקוח לתקשורת עם השרת. לקוח RAS/DUN מספק את האפשרות לחיבור לרשת מרוחקת על ידי שימוש ב-SLIP או PPP. SLIP (Serial Line Internet Protocol) הוא פרוטוקול ישן יותר התומך רק בחיבורי TCP/IP לרשתות מרוחקות, ואינו מספק בדיקת שגיאות או דחיסה. PPP (Point to Point Protocol) הוא היורש של SLIP ונמצא בשימוש נרחב כיום, מכיון שהוא תומך בהעברת נתונים באמצעות מספר פרוטוקולי רשת. PPP גם מספק בדיקת שגיאות מתוחכמת ודחיסה.

למרות שלקוחות RAS/DUN תומכים בחיבורים באמצעות SLIP או PPP, שרת RAS המשולב ב-Windows NT/2000 תומך בחיבורי PPP בלבד.

יש לזכור שאפשרות הגישה מרחוק מציבה סיכונים בתחום האבטחה. רכיב התוכנה RAS של מיקרוסופט כולל מספר אפשרויות להפחתת איום זה ובהן שימוש באבטחת חשבון לקוח של Windows NT, יכולת חיוג חזרה אל המשתמש, והצפנה בין לקוח RAS/DUN לבין שרת RAS.

12

רכיבי קישוריות / רשתות גדולות

כאשר הארגון שלך מתרחב והשימוש ברשת עולה, נוצר מצב שבו קיבולת הרשת הקיימת אינה מספקת. ייתכן שפיסית לא ניתן להאריך את קווי הרשת, או שנפח התעבורה ברשת גבוה מאוד ויש למצוא דרך להקל על הגודש. בכל אחד מהמקרים, קיימות מספר דרכים בהן ניתן להשתמש להרחבת הרשת. פרק זה יתייחס לשימוש בהתקנים הבאים:

- ✯ מגברים (repeaters),
- ✯ גשרים (bridges),
- ✯ מתגים (Switches),
- ✯ נתבים (routers),
- ✯ נתבי-גשר (brouters),
- ✯ שערים (gateways).

הרחבת הרשת המקומית

כאשר הארגון גדל, אחד הצרכים הראשונים עשוי להיות הרחבת הרשת המקומית (LAN) מעבר לתחום הקיים. שני התקנים משמשים למטרה זו:

- ✯ מגברים (repeaters),
- ✯ גשרים (bridges).

מגברים (Repeaters)

מגברים (repeaters) פועלים בשכבה הפיסית של מודל OSI.

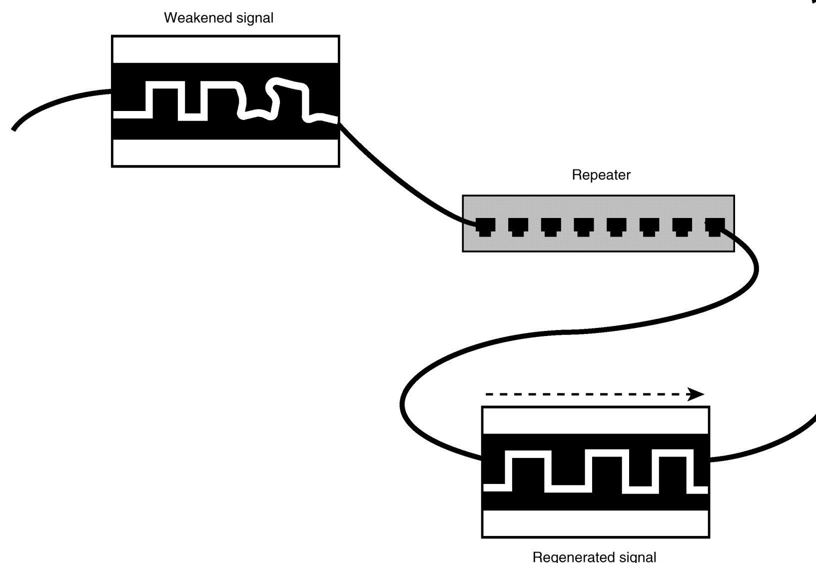
כאשר אות עובר בכבל הוא נתקל בהתנגדות הכבל המחלישה אותו. איכות האות יורדת בהדרגה עד לנקודה שבה לתחנה המקבלת יש קושי לזהות את האות המקורי. תהליך זה, הנקרא **הנחתה** (attenuation), מטיל מגבלות מרחק על התווך הפיסי המשמש ברשתות.

מגברים (repeaters) הם התקנים המקבלים אותות נכנסים מקטע כבל אחד (segment) ומגבירים את עוצמת האות לפני העברתו לקטע כבל אחר. מרבית המגברים אינם מגבירים את האות בלבד לפני שהם שולחים אותו. אילו היו רק מגבירים את העוצמה, אז גם האות וגם הרעש החשמלי בכבל היו מוגברים. על כן, המגברים מקבלים את האות, מפענחים אותו כסדרת סיביות "1" ו-"0" ומייצרים **מחדש** את האות בלבד בקטע הכבל הנוסף. כך, עוצמת האות הנכנסת למקטע הכבל השני תהיה דומה לזו שיצאה מכרטיס ממשק הרשת של המחשב אל הקטע הראשון. תרשים 12.1 מתאר תהליך זה.

המגברים פועלים בשכבה הפיסית (physical) של מודל ייחוס OSI ואינם מודעים לסוג הנתונים, כתובת מנת הנתונים, או לפרוטוקול. הם אינם מבצעים כל תרגום, או סינון של הנתונים עצמם, אלא רק מעבירים אותות מקטע כבל אחד לקטע כבל אחר.



הערה: למרות שסעיף זה מתמקד בתווך הפיסי, המגברים פועלים גם בתווך אלחוטי. לדוגמה, המגברים יכולים לשמש להגדלת התחום של קשר מיקרוגל.



תרשים 12.1: *המגברים מקבלים אות מוחלש ומחוללים אותו מחדש לפני העברתו הלאה ברשת*

מכיון שהמגברים עוסקים רק בשחזור האותות החשמליים או האופטיים, הם אינם יכולים לשמש לחיבור שני מקטעי רשת (Network segment) המשתמשים בארכיטקטורות רשת שונות. לדוגמה, רשת Ethernet אינה יכולה להיות מחוברת לרשת Token Ring באמצעות מגבר. שיטת הגישה, כגון CSMA/CD או העברת אסימון, חייבת להיות זהה **בכל** קטעי הכבל (segment) המחוברים למגבר.

עם זאת, ניתן להשתמש במגברים לחיבור סוגים שונים של תווך פיסי באותה רשת. לדוגמה, רשת Ethernet המשתמשת בזוג שזור יכולה להשתמש במגבר, כגון רכזת, להעברת האות אל כבל קואקסיאלי. אולם, כדי שהעברה זו תצליח, חייבים להשתמש באותה שיטת גישה לתווך **בכל** קטעי הכבל המחוברים.



טיפ: אם השתמשת ברשתות Ethernet מסוג 10BaseT, הפעלת קרוב לוודאי גם במגברים. מרבית הרכזות (Hubs) פועלות גם כמגברים, מלבד רכזות פסיביות שאינן משתמשות במתח חשמלי.

מגברים יכולים להעביר מידע באותה מהירות כמו הרשת, בעיקר משום שהם אינם מעבדים את הנתונים. אולם הם דורשים מעט זמן לחילול מחדש של האות. אם יש מספר מגברים בטור, הזמן הנדרש לחילול מחדש של האות יכול לגרום ל**השהיה** (propagation delay) באות, העלולה להשפיע על התקשורת ברשת. לכן, רוב ארכיטקטורות הרשת מגבילות את מספר המגברים שניתן להשתמש בהם להארכת מקטע רשת. לדוגמה, ברשתות Ethernet מסוג 10Base2, ניתן להשתמש בעד ארבעה מגברים לחיבור חמישה מקטעי רשת.

מגברים מציעים את היתרונות הבאים :

- ✯ מגברים מאפשרים להרחיב את הרשת ולהגדיל את הטווח שלה,
- ✯ מכיון שהם מבצעים מעט עיבוד, אם בכלל, הם אינם משפיעים במידה משמעותית על מהירות הרשת,
- ✯ קיימים מגברים המאפשרים לחבר מקטעי רשת המשתמשים בתווך פיסי שונה.

מכיון שהם אינם "יודעים" דבר אודות מנת הנתונים, מגברים אינם יכולים להפחית או למנוע גודש ברשת. הם רק מעבירים כל מנת נתונים, בין אם היא מכילה נתונים טובים או פגומים. חסרונות נוספים של מגברים הם :

- ✯ למגברים אין כל ידע אודות כתובות או סוגי נתונים, ואינם יכולים לשמש לחיבור מקטעי רשת בעלי ארכיטקטורות שונות,
- ✯ הם אינם עושים דבר להקלת בעיות גודש (congestion) ברשת,
- ✯ קיימת מגבלה על מספר המגברים שבהם ניתן להשתמש ברשת.



רעיון מפתח

מגברים פועלים בשכבה הפיסית של מודל ייחוס OSI לקליטת אותות נכנסים ממקטע רשת אחד, הגברת עוצמת האות והעברתו למקטע רשת אחר. מגברים מטפלים רק באותות חשמליים ואופטיים, ואין להם ידע אודות כתובות ונתונים. לא ניתן להשתמש בהם לחיבור מקטעי רשת בעלי ארכיטקטורות שונות, כמו Token Ring ו-Ethernet.

גשרים (Bridges)

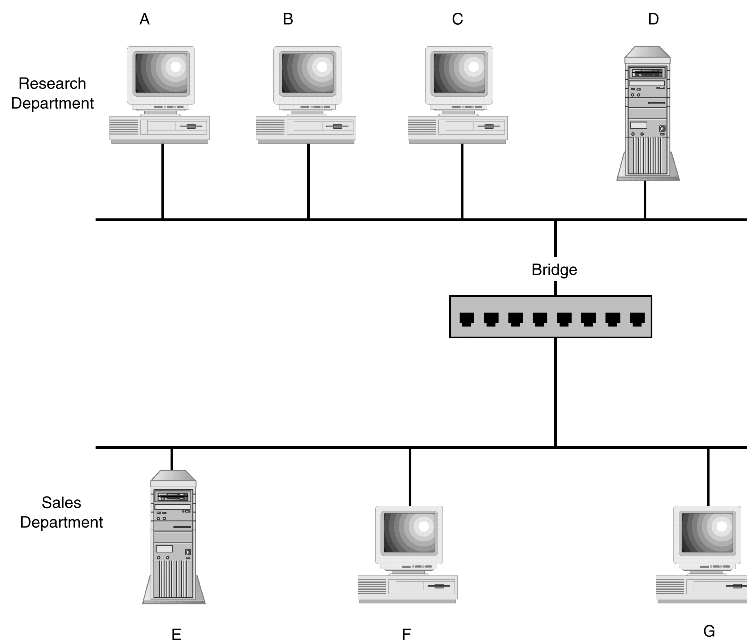
גשרים פועלים בשכבת קישור נתונים במודל ייחוס OSI.

תאר לעצמך שאתה עובד במשרד שבו כל העובדים יושבים בתאים בחדר גדול. כעת תאר לעצמך ששלושה או ארבעה מהם פועלים על פרויקטים משותפים ומדברים זה עם זה על עבודתם. לאורך זמן, שיחותיהם מפריעות לריכוז שלך עד כך שקשה לך לעבוד. פתרון אחד יהיה בניית קיר שיחלק את החדר הגדול לשני חדרים קטנים יותר. העובדים שמדברים ביניהם כל הזמן יהיו בצד אחד של הקיר, ואתה ועמיתיך לעבודה תהיו בצדו האחר. תהיה דלת המאפשרת לך לעבור ולדבר עם האחרים ותאפשר להם לבוא ולבקר אותך, אולם לא תצטרך לשמוע את כל השיחות שמתקיימות ביניהם. הקיר חוסם את העברת הקול בין שני החדרים - מלבד קולות שמיועדים לעבור בין החדרים (לדוגמה, כאשר מישהו פותח את הדלת ומדבר אל תוך החדר האחר).

ברשת מחשבים, **גשרים** (bridges) מבצעים חלוקה ל**מקטעים** (segments), בדומה לזו שהצגנו בקשר לחדרים. כמו מגבר, גם גשר מחבר בין מספר מקטעי רשת ומקבל אותות נכנסים מכל המקטעים. גשרים בודקים את כתובת היעד של המנות לפני העברתן למקטעים אחרים. אם כתובת היעד נמצאת במקטע רשת אחר, הגשר מעביר את האות בדיוק כפי שעושה זאת המגבר. אולם אם כתובת היעד נמצאת במקטע הרשת הנוכחי, הגשר מזהה שאין צורך להעביר את המנה למקטע אחר ונוטש אותה. כתוצאה, ניתן לחלק רשת כך שעומס בחלק מסוים שלה לא ייצור גודש ברשת כולה.

כדוגמה, התבונן ברשת בתרשים 12.2. מחשבים D ו-E הם שרתי קבצים, אולם נמצאים בשתי מחלקות שונות: מחקר ומכירות. אם נשתמש במגבר לחיבור שני מקטעי הרשת, כל מחשב יקבל את כל המנות המועברות על ידי **כל** המחשבים האחרים. כאשר משתמשים ממחלקת מחקר הפועלים במחשבים A, B ו-C יתחילו להעביר קבצי נתונים גדולים הלוך ושוב משרת D, הם ייצרו תעבורת רשת שתאט את התעבורה ברשת **כולה**. משתמשי מכירות הפועלים במחשבים F ו- G יגלו שקצב אחזור קבצים שלהם משרת E איטי מאוד.

אם נשתמש בגשר כמו זה שבתרשים 12.2, מנות העוברות בין מחשבים במחלקת המחקר **לא** יועברו למקטע הרשת של מחלקת מכירות. כאשר מחשב A יבקש קבצים משרת קבצים D, הגשר יקבל את המנה בדיוק כפי שמחשבים B, ו-C יקבלו אותה, אולם הוא יזהה ש-A ו-D נמצאים באותו מקטע רשת וינטוש את המנה מבלי להעביר אותה הלאה. כך, התעבורה הכבדה במחלקת מחקר לא תשפיע על הרשת במחלקת מכירות.



תרשים 12.2: *גשר יכול לחלק רשת למקטעים שונים להקלת העומס הכולל ברשת*

אם מחשב במקטע אחד רוצה לתקשר עם מחשב במקטע אחר, הגשר יזהה זאת ויעביר את המנה. אם החוקר במחשב B זקוק למידע משרת מכירות E, בקשה זו **תשודר** (broadcast) ברשת המחקר ותתקבל גם על ידי הגשר. הגשר יבדוק את המנה, יקבע שהיעד אינו ברשת המחקר, ויעביר אותה הלאה לרשת המכירות. באופן דומה, בקשות מרשת מכירות למשאבים במחלקת מחקר יועברו לרשת של מחלקת מחקר.



רעיון מפתח

חשוב להבין שגשר בודק את כתובת היעד ומשווה אותה לכתובות שהוא יודע כי נמצאות באותה רשת בה נמצא המקור המשדר. אם היעד אינו באותה רשת, הגשר מעביר את המנה. שים לב שהגשר אינו חייב לדעת כי כתובת היעד נמצאת למעשה במקטע אחר; הוא רק יודע שהיעד **אינו** באותו מקטע של המקור.

שימוש בכתובות חומרה

כדי שפעולות אלו יצליחו, צריכה להיות לגשר ידיעה כלשהי על המחשבים שנמצאים בכל מקטע רשת. גשרים פועלים בשכבת קישור הנתונים של מודל ייחוס OSI ויש להם גישה למידע הכתובות בתת-השכבה MAC (בקרת גישה לתווך) בכל מנת נתונים. לכל כרטיס ממשק רשת של מחשב חייבת להיות **כתובת MAC** (MAC address) ייחודית. בדרך כלל ברשתות Ethernet ו- Token Ring, כתובת זו צרובה בכרטיס ממשק הרשת בעת ייצורו. לכרטיסי ממשק רשת ברשת ARCnet מוקצית כתובת מספרית באופן ידני

באמצעות מפסק DIP על הכרטיס. באמצעות אחד ממנגנונים אלה תהיה לכל מחשב כתובת ייחודית שבה ניתן להשתמש ברשת המקומית.

גשרים מבצעים את כל פעולתם באמצעות כתובות MAC אלו, הנקראות גם **כתובות חומרה** (hardware addresses).

סוגי גשרים

גשרים משתמשים ב**גישור שקוף** (transparent bridging) או ב**גישור נתיב-מקור** (source-route bridging) כדי לקבוע איזה מקטע רשת מכיל כתובת חומרה מסוימת.

גשרים **שקופים** (transparent) משמשים ברשתות Ethernet. גשרים אלה, הנקראים גם **גשרים לומדים** (learning bridges), בונים **טבלת גישור** (bridging table) עם קבלת מנות נתונים. כאשר הגשר מופעל לראשונה, טבלת הגישור **ריקה**. כאשר הגשר מקבל מנות ממקטעי הרשת השונים שאליו הוא מחובר, הוא סורק את כתובות המקור והיעד של כל המנות ועוקב מאיזה מקטע רשת הגיעה כל מנה. עם הזמן, הגשר מפתח רשימה מקיפה של הכתובות וכך הוא יכול לדעת להעביר את המנה.

גשרי נתיב-מקור (source-route bridges) משמשים בעיקר בסביבות Token Ring של יבמ וסומכים על מחשב המקור שיספק מידע-נתיב בתוך המנה. גשר מסוג זה אינו דורש כושר עיבוד רב מכיון שמרבית העבודה מבוצעת על ידי מחשב המקור. מחשבי מקור משתמשים ב- explorer packets לקביעת הנתיב הטוב ביותר למחשב מסוים. מידע זה נכלל אחר כך במנה הנשלחת ברשת. כאשר גשר נתיב-מקור מקבל מנה זו, הוא שם לב לנתיב ומשתמש בו עבור מנות הנשלחות לכתובת זו בעתיד.

ללא תלות בסוג הגשר שבשימוש, עליך לדעת שגשרים (bridges) איטיים יותר ממגברים (Repeaters), מכיון שעליהם לבדוק את הכתובת של כל מנת נתונים. מצב זה אינו אמור להוות בעיה אם הרשת מחולקת נכון למקטעים, כך שמשתמשים שצריכים לתקשר זה עם זה לעיתים קרובות נמצאים באותו צד של הגשר. על ידי סינון מנות נתונים, גשרים יכולים להגביר מהירות כוללת של הרשת על ידי הפחתת הגודש (Reducing Congestion).

אולם, גשרים אינם מפחיתים גודש רשת הנוצר על ידי **מנות שידור לכל** (broadcast packets). רוב מנות הנתונים הנשלחות ברשת נשלחות ממחשב אחד לאחר. אולם קיימים מצבים שבהם מחשב צריך למסור מידע לכל המחשבים האחרים ברשת. כדי לעשות זאת, המחשב שולח **מנת שידור לכל** אל הרשת. כאשר כל המחשבים האחרים ברשת מקבלים מנה זו, הם קוראים ומעבדים אותה, כאילו היתה מכותבת אליהם ישירות.

מנות שידור לכל יכולות להועיל ברשת. למעשה, קיימים פרוטוקולי רשת כגון NetBEUI המסתמכים על העברת מנות מסוג זה. עם זאת, שימוש מוגזם במנות אלו יכול לפגוע במידה ניכרת במהירות הרשת. היכולת לשלוח מנות שידור לכל יכולה להוביל גם לאסון, אם כרטיס ממשק רשת מתקלקל ומתחיל למלא את הרשת בשידורים לכל. מצב זה, המכונה **סערת שידור לכל** (broadcast storm), עלול להפיל את הרשת. גשרים אינם מסייעים במצב זה, מכיון שהם מעבירים כל מנת שידור לכל.



רעיון מפתח

גשרים מעבירים את כל מנות שידור לכל. בנוסף, כאשר גשר נתקל בכתובת יעד לא מוכרת, פעולת ברירת המחדל היא העברת המנה לכל מקטעי הרשת האחרים.

גישור בין רשתות שונות

כמו מגברים, גם גשרים יכולים לחבר בין מקטעי רשת המשתמשים בתווך פיסי שונה. למשל, גשר יכול לחבר בין מקטע רשת 10BaseT Ethernet ל- 10Base2 Ethernet.

קיימים **גשרי תרגום** (translation bridges) המיועדים להתייחס להמרה בין ארכיטקטורות שונות. לדוגמה, קיימים גשרי תרגום המאפשרים חיבור רשתות Ethernet ו- Token Ring, ויש להם כניסת Ethernet וכניסת Token Ring. לצמתי Ethernet גשרים אלה נראים כגשרים שקופים (transparent) ומקבלים העברה של מסגרות נתוני Ethernet. עבור צמתי Token Ring הם נראים כגשרי ניתוב-מקור (source-route) ומקבלים מסגרות Token Ring. גשרים אלה גם מתרגמים מסגרות Ethernet למסגרות Token Ring ולהיפך. באופן דומה, קיימים גשרים המתרגמים מסגרות בין Ethernet ובין FDDI.

יתרונות וחסרונות

גשרים מציעים יתרונות רבים, ביניהם:

- ✯ גשרים יכולים לפעול כמגברים ולהרחיב את הרשת לטווחים גדולים יותר,
- ✯ גשרים יכולים להגביל את זרימת התעבורה בין מקטעי רשת ולהקל על גודש,
- ✯ גשרים יכולים לחבר מקטעי רשת המשתמשים בתווך פיסי שונה,
- ✯ גשרים מסוג גשרי תרגום יכולים לחבר רשתות בעלות ארכיטקטורה שונה.

אולם לגשרים יש גם חסרונות, שביניהם:

- ✯ מכיון שגשרים בודקים כתובות חומרה, הם איטיים יותר ממגברים,
- ✯ מנות שידור לכל המיועדות לכל המחשבים ברשת, מועברות על ידי גשרים לכל מקטעי הרשת,
- ✯ גשרים יקרים ומורכבים יותר ממגברים.



רעיון מפתח

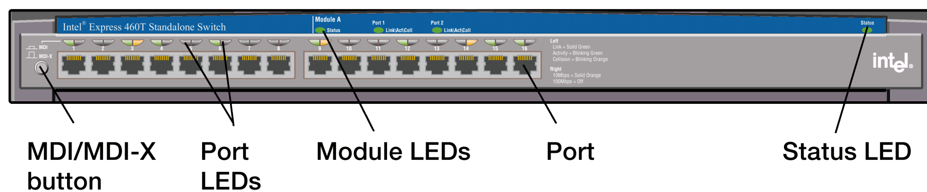
גשרים פועלים בשכבת קישור הנתונים של מודל ייחוס OSI ומשמשים בעיקר לחלוקת רשת למקטעים להפחתת התעבורה ברשת.

מתגים (Switches)

השימוש בהתקני תקשורת הידועים כ**מתגים** (Switches) הופך לנפוץ ברשתות תקשורת ובתעשיית ההיי-טק כולה.

כעיקרון, מתג נראה דומה מאוד לרכזת (Hub). אתה מחבר מחשבים למתג בדיוק כפי שאתה עושה זאת לרכזת, ולמתבונן מהצד יהיה קשה להבדיל בין השניים.

במבט מעמיק ניתן להבחין כי קיים הבדל מהותי בין מתג (Switch) לבין רכזת (Hub). זכור שכאשר מגיע אות (signal) ליציאה (port) ברכזת, הוא מחולל מחדש בכל מעבר ביציאה כלשהי ברכזת. בניגוד לכך, מתג (Switch) משמש כגשר (Bridge) ולומד את כתובת הרשת של כל מחשב המחובר לכל יציאה בו. כאשר מגיע אות לאחת היציאות, כותרת הנתונים (Data Header) נבדקת ואז ממותגת ישירות ובמדויק רק ליציאה המחוברת למחשב היעד.



תרשים 12.3: *מתג Switch*

היתרון הגדול ביותר של גישה זו הוא, שלא כמו במקרה הרכזת, ניתן לשדר למספר מחשבים בו-זמנית. אם מחשב 2 צריך לשלוח נתונים למחשב 4, יקשר המתג את יציאות 2 ו-4. במקביל, מחשב 3 צריך לשלוח נתונים למחשב 8 ומחשב 1 צריך לשלוח נתונים למחשב 5. כל שטפי הנתונים הללו יכולים להישלח בו-זמנית, מפני שאינם משתמשים באותן יציאות. כעת, אם מחשב 7 מעוניין גם הוא לשלוח נתונים למחשב 4, המתג ממתג את הנתונים בין יציאות 2 ו-7 (השולחות), ומאפשר לכל אחת בתורה לשלוח נתונים למחשב 4.

בנוגע לכתובות בהן הוא משתמש, המתג ישתמש בדרך כלל בשכבה 2 (Hardware, חומרה - Ethernet או Toking Ring, למשל) או בשכבה 3 (רשת, Network - IP או IPX), תלוי ביצרן. מתגים מיישמים את כל בדיקות המנות שלהם בחומרה ופועלים במהירויות גבוהות במיוחד.

שילוב רשתות (Internetworking)

רשת משולבת (internet או internetwork) מורכבת משתי רשתות עצמאיות או יותר, המחוברות יחד, אך ממשיכות לתפקד כל אחת בנפרד. דוגמה לכך היא רשת Token Ring ורשת Ethernet ה**מחוברות יחד** (interconnected), כך שמשתמשים בכל אחת מהן יכולים לגשת למשאבים ברשת האחרת. שתי הרשתות ממשיכות לתפקד כרשתות נפרדות, אולם משתמשים יכולים להעביר נתונים בין שתיהן. הרשת המשולבת המוכרת ביותר בשימוש כיום היא ללא כל ספק **רשת האינטרנט העולמית**, המורכבת כולה מרשתות קטנות יותר המחוברות זו לזו.

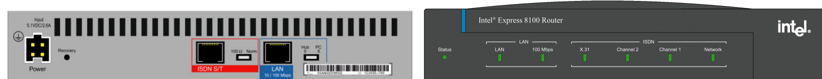
משימת החיבור בין רשתות שונות מבוצעת על ידי התקן **שילוב רשתות** (internetworking device). בסעיף זה נלמד אודות שלושה התקנים מסוג זה:

- נתבים (routers),
- נתבי-גשר (brouters),
- שערים (gateways).

נתבים (Routers)

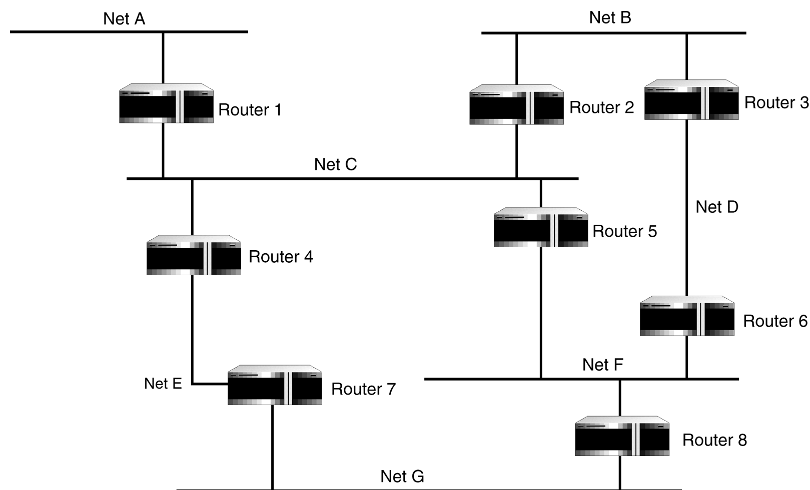
נתבים פועלים בשכבת הרשת (Network) של מודל OSI. גשרים פועלים כראוי לחיבור מספר רשתות קטנות. אולם, ככל שהרשת גדלה במורכבותה מתחילות לבלוט גם מגבלותיהם. לדוגמה, ככל שרשתות חיוניות יותר לפעולות יומיומיות גדל הרצון למצוא מספר נתיבים בין מקטעי רשת, כך שנתונים יוכלו לזרום בין מקטעי הרשת השונים גם כאשר נתיב אחד כושל. גשרים אינם פועלים היטב עם מספר נתיבים ובמקרים אחדים הם עלולים ליצור מצבים שבהם מנות "מטיילות" ברשת במעגלים אינסופיים. גם לו יכלו הגשרים להתמודד עם מספר נתיבים, הם אינם כוללים מנגנון הקובע איזה נתיב הוא הטוב ביותר.

נתבים (routers) הם התקנים שיכולים לחבר רשתות שונות כדי ליצור **רשת משולבת** (internetwork) מורכבת. כמו גשרים, גם נתבים יכולים לשמש לחיבור פשוט בין מקטעי רשת וסינון התעבורה בה. אולם, שלא כמו גשרים, תהליך סינון זה משתמש בכתובות רשת (ולא בכתובות חומרה).



תרשים 12.4: *נתב (Router), במקרה זה נתב לחיבור לאינטרנט*

כפי שמוצג בתרשים 12.5, נתבים יכולים לשמש ליצירת רשתות שבהן יש מספר נתיבים בין מקטעי הרשת. לכל מקטע רשת, הנקרא גם **רשת משנה** (subnetwork או **subnet**), מוקצית כתובת רשת. בנוסף, לכל צומת מחשב ברשת המשנה מוקצית כתובת מסוימת. על ידי שימוש בשילוב זה של כתובות רשת וצמתים, הנתב יודע ל**נתב** (route) מנות נתונים מכתובת מקור לכתובת יעד שנמצאת במקום אחר ברשת.



תרשים 12.5: *נתבים יכולים לשמש ליצירת רשתות מורכבות*

כדי להשיג את יכולת הניתוב שהצגנו, הנתב חייב להוריד את מידע שכבת קישור הנתונים ממנת הנתונים ולבחון את כתובת היעד של שכבת הרשת שנמצאת בתוכה. כל מנת נתונים המועברת מכילה את כתובת רשת היעד ואת כתובת צומת היעד המתאימות לפרוטוקול הרשת שבשימוש.

לאחר שהנתב מקבל כתובת יעד של מנה, הוא משווה את הכתובת ל**טבלת הניתוב** (routing table) הפנימית שלו, כדי לקבוע באיזה **נתיב** המנה תעבור. הנתב אורז מחדש את מנת הנתונים על ידי מידע שכבת קישור נתונים המתאים לנתיב שבו תעבור המנה.

היתרון בגישה זו הוא שנתבים יכולים לשלוח מידע **בין ארכיטקטורות** רשת שונות. לדוגמה, מנה שהתקבלה מרשת Ethernet תוכל לעבור ברשת Token Ring. הנתב מסיר את מסגרת הנתונים של Ethernet, בודק את המנה כדי לקרוא את כתובת הרשת, אורז את הנתונים מחדש במסגרת Token Ring ושולח אותה אל רשת Token Ring.

שים לב שיכולים להיות הבדלים במהירות בעת ניתוב בין ארכיטקטורות שונות. לדוגמה, רשתות Ethernet משתמשות במסגרת נתונים בגודל 1,500 בתים בערך, ואילו מסגרות Token Ring יכולות להיות בגודל שבין 4,000 ל-18,000 בית בערך. העברת מנות מ-Ethernet ל-Token Ring פשוטה: הנתב לוקח את הנתונים ממנת Ethernet ומכניס אותם למנת Token Ring. אולם בשידור בכיוון הפוך, הנתב חייב לארוז מחדש נתונים ממנת Token Ring למספר מנות Ethernet לפני שהוא משדר אותן, מכיון שמסגרת נתונים ב- Token Ring גדולה יותר.

הבדל גדול בין גשרים לנתבים נמצא בדרך שבה הם מתמודדים עם כתובות לא מוכרות. כאשר גשר מזהה מנה שכתובת היעד שלה אינה מוכרת, הוא מעביר אותה לכל מקטעי הרשת המחוברים, מלבד למקטע שממנו היא הגיעה אליו. נתב, לעומת זאת, מצפה שיוכל לזהות את כתובת הרשת ושולח רק מנות שעבורן יש לו כתובת ברורה. אם כתובת יעד אינה תואמת אף רשומה בטבלת הניתוב, המנה מושלכת. בנוסף, מנות שניזוקו מושלכות על ידי הנתבים, למרות שגשרים היו מעבירים אותן.

נתבים גם משליכים מנות שידור לכל (broadcast packets), ומקטינים את ההשפעות של סערות שידור לכל (broadcast storm).



רעיון מפתח

עם קבלת מנת שידור לכל (broadcast packets) או מנה עם כתובת יעד לא מוכרת, **גשרים מעבירים** (forward) את המנה, **ונתבים משליכים** (discard) אותה.



הערה: העובדה שנתבים משליכים מנת שידור לכל (broadcast packets) עלולה להשפיע על מבנה הרשת שלך. לדוגמה, זכור לך שברשת TCP/IP ניתן להקצות כתובות באופן דינמי באמצעות שרת DHCP. כאשר מחשב מופעל, הוא משדר מנת שידור לכל ומבקש הקצאה של כתובת IP משרת DHCP. מכיון שנתבים (routers) אינם מעבירים מנות שידור לכל, תצטרך שרת DHCP בכל רשת משנה (subnet) ברשת המשולבת (שים לב שניתן להגדיר נתבים אחדים להעברת בקשות DHCP בהתאם לתהליך המוגדר ב- RFC 1542).

טבלת הניתוב של נתב שונה מטבלת גישור בכך שגשר עוקב אחר **כתובות חומרה** במקטעים הקשורים אליו, ואילו נתב עוסק ב**כתובות רשת** בלבד. גשר יודע את כתובות המחשבים עצמם במקטעי הרשת המחוברים אליו וגם את כתובות המחשבים במקטעי רשת רחוקים, ואילו נתב יודע רק את הכתובות של רשתות אחרות ושל הנתבים המטפלים בהן.

סוגי נתבים

ניתן לבנות טבלת ניתוב בשתי דרכים: על ידי **ניתוב סטטי** (static routing) או על ידי **ניתוב דינמי** (dynamic routing).

נתבים סטטיים (static routers) דורשים שמנהל רשת יגדיר ידנית את טבלת הניתוב, שבה כל נתיב חייב להיות מוזן ידנית. הנתב ישתמש תמיד באותו נתיב לשידור מנות לכתובת רשת מסוימת, גם אם אין זה בהכרח הנתיב הקצר ביותר. אם אין נתיב לכתובת רשת מסוימת, לא ניתן לספק את המנה.

נתבים דינמיים (dynamic routers) לעומת זאת, משתמשים בתהליך **גילוי** (discovery) לבירור המידע אודות נתיבים זמינים. נתבים אלה מתקשרים עם נתבים אחרים ומקבלים כל העת טבלאות ניתוב מעודכנות מנתבים אחרים. אם קיימים מספר נתיבים בין שתי רשתות, נתבים דינמיים יכולים לבחור את הנתיב הטוב ביותר עבור כל מנה. נתבים דינמיים בוחרים את הנתיב הטוב ביותר באחת משתי דרכים:

- **אלגוריתם וקטור-מרחק** (distance-vector algorithm) מחשב את ה**עלות** של כל נתיב על פי מספר הנתבים (או **קפיצות** - hops) בין שתי רשתות. הנתיב שבו תועבר מנה מסוימת ייקבע על פי הנתיב בעל העלות הנמוכה ביותר. פרוטוקול RIP (Routing Information Protocol), המשמש הן ברשתות TCP/IP והן ברשתות IPX/SPX, הוא דוגמה לאלגוריתם מסוג זה.

* **אלגוריתם מצב-קישור** (link-state algorithm) מתחשב בפקטורים נוספים, כגון תעבורת רשת, מהירות חיבור ועלויות מוקצות בעת חישוב הנתיב הטוב ביותר. נתבים המשתמשים באלגוריתם מסוג זה דורשים עוצמת חישוב גבוהה יותר ומאפשרים העברת מנות יעילה. OSPF (Open Shortest Path First) הוא אלגוריתם מצב-קישור שנמצא בשימוש ברשתות TCP/IP רבות.

נתבים דינמיים קלים יותר לתחזוקה מאשר נתבים סטטיים, אולם העדכון השוטף של טבלאות ניתוב יוצר תעבורת רשת נוספת.

פרוטוקולים מנותבים (routable)

חיסרון אחד של נתבים הוא שהם פועלים רק עם פרוטוקולי רשת מנותבים שמנגנון הקצאת כתובות הרשת שלהם תומך בשיטה כלשהי של חלוקת הרשת למקטעים. פרוטוקולים **מנותבים** (routable) הם:

* TCP/IP.
* IPX/SPX (Novell NetWare),
* DEC/Net,
* OSI,

פרוטוקולים **חסרי ניתוב** (non-routable) הם:

* DLC (משמש עם מדפסות רשת HP ומחשבים גדולים של יבמ),
* LAT (Digital Equipment Corporation),
* NetBEUI (מיקרוסופט).

יתרונות וחסרונות

נתבים מציעים יתרונות רבים, ביניהם:

* נתבים יכולים לחבר בין רשתות המשתמשות בארכיטקטורות רשת ובשיטות גישה לתווך שונות, כגון Ethernet ו- Token Ring,
* כאשר יש מספר נתיבים על פני הרשת, נתב יכול לבחור בנתיב הטוב ביותר ולהשתמש ביעילות במשאבי רשת,
* נתבים יכולים להפחית גודש רשת, מכיון שלא כמו גשרים, הם אינם מעבירים הודעות שידור לכל, או מנות נתונים פגומות.

לנתבים יש גם חסרונות, ביניהם:

* נתבים יקרים ומורכבים יותר מאשר גשרים ומגברים,
* נתבים פועלים רק עם פרוטוקולי רשת מנותבים,
* בשימוש בניתוב דינמי, עדכונים שוטפים של מידע ניתוב יוצרים תעבורת רשת נוספת,

★ נתבים איטיים יותר מגשרים מכיון שהם זקוקים ליותר פעולות עיבוד של מנות הנתונים.



רעיון מפתח

נתבים פועלים בשכבת רשת התקשורת של מודל ייחוס OSI ומחברים רשתות באמצעות פרוטוקולי תקשורת. הם קובעים את הנתיב הטוב ביותר למעבר מנת נתונים, ושולחים את המנה ליעד המתאים. מכיון שנתבים פועלים עם פרוטוקולי רשת, הם יכולים להעביר מנות בין ארכיטקטורות רשת שונות.

נתבי-גשר (Brouters)

נתבי-גשר (brouters) פועלים בשכבת קישור נתונים ובשכבת הרשת במודל OSI.

נתבי-גשר הם התקנים היברידים המשלבים היבטים של גשרים ונתבים כאחד. כאשר נתבי-גשר מקבלים מנות נתונים המשתמשות בפרוטוקולים מנותבים, הם מתפקדים בדיוק כמו נתבים ומנתבים את המנות האלו ליעד המתאים. אולם, כאשר נתבי-גשר מקבלים מנות נתונים המשתמשות בפרוטוקולים חסרי ניתוב, הם פועלים כגשר ומעבירים את המנה על פי כתובות החומרה. כדי להשיג זאת, משתמשים נתבי-גשר הן בטבלת גישור (המבוססת על כתובות חומרה) והן בטבלאות ניתוב עבור הפרוטוקולים בשימוש ברשת.

בדרך כלל נתבי-גשר נמצאים ברשתות המשתמשות בתערובת של פרוטוקולים מנותבים וחסרי ניתוב. לדוגמה, אם ברצונך להקטין את תעבורת הרשת ברשת גדולה המשתמשת הן ב-TCP/IP והן ב-NetBEUI, נתבים או גשרים בלבד לא יספקו פתרון. גשרים יאפשרו לחלק את הרשת למספר מקטעים, אולם יעבירו מנות שידור לכל ממקטע אחד אל כל המקטעים האחרים. נתבים יאפשרו לחלק את הרשת, כך שכתובות TCP/IP יועברו רק במקטעי המקור והיעד שלהם, וימנעו תעבורה במקטעים האחרים. אולם מכיון ש-NetBEUI הוא פרוטוקול חסרי ניתוב, המשתמשים בו לא יוכלו לתקשר מעבר למקטע הרשת שלהם.

נתבי-גשר מאפשרים לפתור בעיה זו על ידי ניתוב מנות TCP/IP וגישור מנות NetBEUI. למרות שהתוצאה היא עדיין שמנות NetBEUI מועברות לכל המקטעים, ניתן בכל זאת להקטין את תעבורת הרשת במידה מסוימת על ידי מניעת שידורים של מנות TCP/IP לכל המקטעים.

נתבי-גשר יכולים להוות כלי מצוין לחלוקת רשתות מסוימות למקטעים. בנוסף, הם יכולים להיות כדאיים יותר כלכלית במצבים מסוימים מאשר גשרים ונתבים נפרדים. אולם, הם בדרך כלל יקרים ומורכבים יותר מהתקני רישות אחרים, ולכן נמצאים בשימוש מוגבל בלבד.



רעיון מפתח

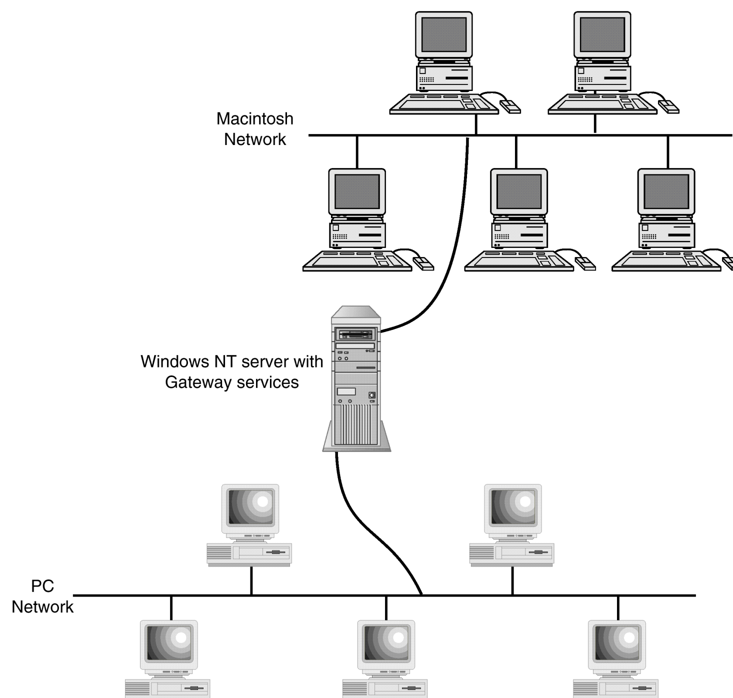
נתבי-גשר (brouters) הם התקנים המתפקדים הן בשכבת רשת התקשורת והן בשכבת קישור הנתונים של מודל ייחוס OSI ומשלבים רכיבים של גשרים ונתבים. הם מנתבים מנות המשתמשות בפרוטוקולים מנותבים ומגשרים מנות המשתמשות בפרוטוקולים חסרי ניתוב.

שערים (gateways)

שערים פועלים בשכבות הגבוהות משכבת הרשת (Network) ובדרך כלל בשכבת היישום במודל OSI. **שער** (gateway) מתרגם מידע בין שתי ארכיטקטורות רשת, או תצורות נתונים שונות לחלוטין. דוגמה תהיה שער המאפשר לרשת תקשורת מקומית של TCP/IP לתקשר עם מערכת מחשב גדול (mainframe) המשתמש ב-SNA (Systems Network Architecture) של יבמ. דוגמה נוספת תהיה שער הממיר דואר אלקטרוני מ- Microsoft Mail לפרוטוקול SMTP (Simple Mail Transport Protocol) להעברה ברשת.

בשעה שנתבים פועלים בשכבת רשת התקשורת של מודל ייחוס OSI ויכולים לנתב מנות המשתמשות באותו פרוטוקול (כגון IP או IPX) על פני רשתות ללא קשר לארכיטקטורת הרשת הבסיסית (Token Ring ,Ethernet), שערים יכולים לנתב נתונים על פני רשתות המשתמשות בפרוטוקולים שונים. שערים יכולים לשנות את תצורת הנתונים עצמם, ואילו נתבים יכולים רק לארוז את הנתונים מחדש בתצורות מסגרת נתונים שונות.

לדוגמה, Windows NT Server כולל Services for Macintosh. שירות זה מאפשר ללקוח רשת Windows של מיקרוסופט המשתמש ב-NetBEUI לתקשר עם מחשבי מקינטוש המשתמשים ב-AppleTalk דרך Windows NT Server. תוכנת השער מאפשרת לשרתי הקבצים ולמדפסות של מקינטוש להיראות ללקוחות Windows של מיקרוסופט כאילו היו ברשת המחשבים האישיים. באופן דומה, השער מאפשר למחשבי מקינטוש לראות שרתי קבצים ומדפסות של רשת המחשבים האישיים, כאילו היו ברשת מקינטוש. השער מטפל בכל התרגום של נתונים מ-NetBEUI ל-AppleTalk וחזרה, כפי שמוצג בתרשים 12.6.



תרשים 12.6: *Windows NT Server המריץ Services for Macintosh יכול לחבר בין רשתות מחשבים אישיים לרשתות מקינטוש*

כאשר מנות נתונים מגיעות לשער, תוכנת השער מסירה את מידע הרישות וממשיכה להעביר את הנתונים במעלה שכבות מודל OSI עד שהם מגיעים לשכבה שבה ניתן לתרגם אותם. לאחר תרגום הנתונים לתצורה הדרושה עבור היעד, השער אורז אותם מחדש באמצעות **פרוטוקולי הרשת של מערכת היעד** ושולח אותם אל היעד.

מכיון ששערים עוסקים בדרך כלל בתרגום נתונים, הם פועלים בשכבות הגבוהות יותר של מודל OSI. חלקם עשוי לפעול בשכבת רשת התקשורת או בשכבת המושב, אולם רובם פועלים בשכבת היישום.

שערים מתמקדים בדרך כלל במשימה אחת ובמקרים רבים דרוש להם **מחשב ייעודי**. לרוב הם יקרים יותר מאשר התקני שילוב רשתות אחרים, בנוסף להיותם קשים יותר להתקנה ואיטיים יותר מהתקנים אחרים, כמו נתבים, למשל.

יתרונות שערים כוללים בין השאר:

- שערים יכולים לקשר בין מערכות שונות לחלוטין,
- הם מתמחים במשימה אחת ויכולים לבצע אותה היטב.

חסרונות שערים כוללים בין השאר:

- שערים בדרך כלל יקרים יותר מהתקנים אחרים,
- במקרים רבים שערים מסובכים יותר להתקנה ולהגדרה; בגלל העיבוד הדרוש לתרגום הנתונים, שערים עלולים להיות איטיים.



הערה: שערים מתפקדים בשכבת היישום ובשכבות עליונות אחרות של מודל ייחוס OSI כדי לקשר מערכות המשתמשות בפרוטוקולים, או בתצורות נתונים שונות לחלוטין.

סיכום

בעת הרחבת רשת או חיבור של מספר רשתות, ניתן להשתמש בהתקנים מסוגים שונים.

מגברים (repeaters) מגדילים את הטווח שרשת יכולה לכסות. מגבר מקבל אות נכנס, מפענח אותו כמחרוזת של סיביות "1" ו-"0" ושולח אותו מחדש למקטע כבל אחר. מגברים אינם יודעים דבר אודות הנתונים ופועלים רק עם האותות שנמצאים למעשה על תווך הרשת.

גשרים (bridges) יכולים לפעול כמגברים להרחבת רשת ולחיבור מקטעי רשת, אולם הם גם יכולים לסנן תעבורת רשת להפחתת גודש. גשרים פועלים עם כתובות חומרה המוקצות לכרטיס ממשק רשת בדרך כלשהי. גשר קורא את כתובות המקור והיעד של כל מנת נתונים נכנסת ומשווה אותן לאלו ש**בטבלת גישור** (bridging table). אם כתובות המקור והיעד נמצאות באותו מקטע רשת, מנת הנתונים מושלכת. אם הכתובות נמצאות במקטעי רשת שונים והגשר יודע באיזה מקטע נמצא היעד, מנת הנתונים מועברת למקטע זה בלבד. אם כתובת היעד אינה ידועה, הגשר מעביר את מנת הנתונים לכל מקטעי הרשת, מלבד זה שממנו היא הגיעה.

גשרים יכולים לפעול בשכבת קישור הנתונים של מודל OSI, וכמעט בכל המקרים הם דורשים ששיטות הגישה יהיו זהות בכל מקטעי הרשת.

בשעה שגשרים פועלים עם כתובות חומרה, **נתבים** (routers) פועלים עם כתובות פרוטוקול רשת ויכולים להעביר נתונים על פני רשתות המשתמשות בשיטות גישה שונות (Token Ring ,Ethernet). כאשר נתב מקבל מנה, הוא בוחן את כתובת פרוטוקול הרשת, משווה את כתובת היעד ל**טבלת ניתוב** (routing table), קובע את הנתיב הטוב ביותר להעברת מנת הנתונים ושולח אותה אל היעד. שלא כמו גשר, נתב יכול לבחון את מידע הכותרת של מנה, והוא אינו מעביר מנות שידור לכל, או מנות משובשות.

נתבים פועלים בשכבת רשת התקשורת של מודל OSI ויכולים לפעול רק עם פרוטוקולי רשת מנותבים כגון TCP/IP ו-IPX/SPX. מנות המשתמשות בפרוטוקולים חסרי ניתוב כגון NetBEUI ו-DLC אינן יכולות לעבור דרך הנתב והן מושלכות.

נתבי-גשר (Brouters) הם התקנים היברידים המשלבים תכונות של גשרים ונתבים ונמצאים רק ברשתות הנזקקות לפרוטוקולים שונים. כאשר מתקבלת מנה המשתמשת בפרוטוקול מנותבים, נתב-גשר פועל כנתב ומנתב את המנה ליעד המתאים; כאשר מתקבלת מנה המשתמשת בפרוטוקול חסר ניתוב, נתב-גשר מתפקד כגשר וקובע לאן להעביר את המנה על פי כתובות חומרה.

שערים (gateways) הם התקנים המתרגמים מידע בין שתי ארכיטקטורות, או תצורות נתונים שונות לחלוטין. שערים פועלים בשכבות העליונות של מודל ייחוס OSI, ושלא כמו נתבים או גשרים, הם יכולים לשנות את תצורת הנתונים עצמם. דוגמאות לשערים כוללות מערכות המשמשות להמרת הודעות מתצורת דואר אלקטרוני אחת לאחרת ומערכות המאפשרות לרשתות מחשבים אישיים מקומיות לתקשר עם מערכות מחשבים מרכזיים.

טבלה 12.1 מפרטת את ההתקנים שהצגנו בפרק זה, את שכבת מודל OSI שבה פועל כל התקן, דוגמה לסוג האות או הפרוטוקול שההתקן פועל אתם ושימוש אופייני ברשת.

טבלה 12.1: *השוואה בין התקנים המשמשים להרחבה וקישור בין רשתות*

התקן	**שכבת OSI**	**פועל עם**	**שימוש אופייני**
מגבר (repeater)	שכבה פיסית	אותות חשמליים	מאריך מקטעי רשת מקומית (LAN).
גשר (bridge)	שכבת קישור הנתונים	כתובות חומרה	מגדיל טווח רשתות מקומיות, מסנן תעבורת רשת על פי כתובות חומרה, מפצל רשת.
נתב (router)	שכבת הרשת	פרוטוקולים מנותבים (IPX ,IP)	מחבר בין רשתות, קובע נתיבים עדיפים, שולח מנות על פי כתובת רשת לארכיטקטורות שונות.
נתב-גשר (brouter)	שכבת הרשת ושכבת קישור הנתונים	פרוטוקולים מנותבים וחסרי ניתוב	פועל כנתב וכגשר.
שער (gateway)	שכבת היישום ושכבות אחרות מעל שכבת הרשת	פרוטוקולים שונים, דואר אלקטרוני, יישומים	מחבר בין מערכות שונות על ידי תרגום פרוטוקולים ונתונים לפרוטוקולים שונים.

13

רשתות מרחביות (WANs)

עד עתה התמקדנו בנושאים הסובבים את רשת התקשורת המקומית (LAN). פרק זה יביא אותך אל מעבר לרשת המקומית וידון בשיטות הקיימות לחיבור הרשת המקומית שלך אל רשתות מקומיות אחרות. עד סוף פרק זה תדע:

- להבחין בין רשתות מיתוג מעגלים (circuit-switching) לבין רשתות מיתוג מנות (packet switching),
- לזהות את הציוד המשמש לקישוריות דיגיטלית,
- לתאר את הטכנולוגיות השונות המקובלות לחיבורי WAN.

סקירת קישוריות רשת מרחבית (Wide Area Networks)

באזור גיאוגרפי קטן מאוד, תמצא שרשתות מקומיות (LAN) פועלות היטב. על ידי שימוש בתווך פיסי מתאים והתקני קישוריות, כגון נתבים וגשרים (Routers and Bridges), ניתן להרחיב את הרשת המקומית שבבניין המשרדים או במפעל, על ידי חיבור מספר רשתות מקומיות. לדוגמה, אם לארגון שלך יש משרדים במספר בניינים קרובים זה לזה, ניתן לחבר את הרשתות המקומיות שבכל בניין ליצירת רשת מקומית גדולה יותר.

בסופו של דבר, תגיע לנקודה שבה לא ניתן יותר להאריך את תווך הרשת המקומית. רוב סוגי התווך הפיסי שנידונו בספר זה יכולים לכסות מרחק מירבי של 500 מטרים. באמצעות כבלי סיב-אופטי ניתן להאריך מרחק זה עד שני ק״מ, אולם העלות עלולה להיות מרתיעה.

כאשר רוצים להרחיב את הרשת אל מעבר לגבולות הרשת המקומית, יש לחפש טכנולוגיות המאפשרות ליצור רשת המשתרעת על פני מרחקים גדולים. רשת מסוג זה נקראת **רשת תקשורת מרחבית - WAN** (Wide Area Network), בקצרה: **רשת מרחבית**.

רשת מרחבית יכולה להתפרש על פני אזור, מדינה, ארץ, או סביב לעולם. הטכנולוגיות הכרוכות בהקמתה דומות באופן עקרוני, ללא קשר למרחק. מן הבחינה הפיסית, רשת מרחבית יכולה לכלול מספר רשתות מקומיות המחוברות ביניהן בקווי תקשורת במהירות גבוהה (המכונים לעיתים **קווי WAN**, **ערוצי WAN** - WAN links). גשרים, נתבים והתקני קישוריות אחרים יבטיחו שכל הנתונים יועברו כהלכה באמצעות קווי התקשורת. רשת מרחבית המעוצבת כראוי, אמורה לאפשר למשתמשי הרשת שלך לגשת למשאבי רשת מעבר לקשרי WAN באותה קלות כמו למשאבים הנמצאים ברשת המקומית.

בכל הנוגע לקווים עצמם, רוב הארגונים אינם בעליהם של קווי WAN הפיסיים. יהיה זה יקר מדי לארגון לרכוש את כל הכבלים הפיסיים לטווחים רחוקים, לחבר אותם בין משרדים, ואז להמשיך ולתמוך בהם. במקום זאת, רוב קשרי WAN חכורים מספקי שירות שהתווך הפיסי נמצא בבעלותם והם גם אחראים לתחזוקה.

ספקי שירותים כיום כוללים את חברת הטלפון המקומית, חברות המספקות **שירותי חוץ** (long distance) מוכרות, וחברות המתמחות בתמסורת נתונים (data transmission).

קווי WAN כוללים למעשה אחת מהטכנולוגיות:

- קווי טלפון בחיוג (dial-up),
- קווי טלפון דיגיטליים ייעודיים (dedicated),
- רשתות מיתוג-מנות (packet switching).

כל אחת מהטכנולוגיות תידון בפירוט בפרק זה. אולם תחילה עליך להבין את סוגי הקווים הזמינים.

סוגי חיבורים

אם תרכוש כבל ותעביר אותו פיסית בין שני בניינים, יהיה לך חיבור פרטי. כפי שנאמר בסעיף הקודם, רוב הארגונים אינם יכולים להרשות זאת לעצמם ובוחרים לחכור קווים מספק שירותים. החיבור החכור יכול להיות אחד משני סוגים: חיבור ייעודי, או חיבור באמצעות רשת ממותגת כלשהי.

חיבורים ייעודיים (Dedicated)

בחיבור ייעודי הקו מוחכר לך בלבד, Full Time. **חיבור ייעודי** (dedicated connection) כרוך בחיבור קבוע, שפתוח כל הזמן בין שתי נקודות. למעשה, השירות זהה לזה שהיה אילו העברת את הכבל בעצמך. ההבדל הוא שהכבל בבעלות מישהו אחר האחראי גם על תחזוקתו.

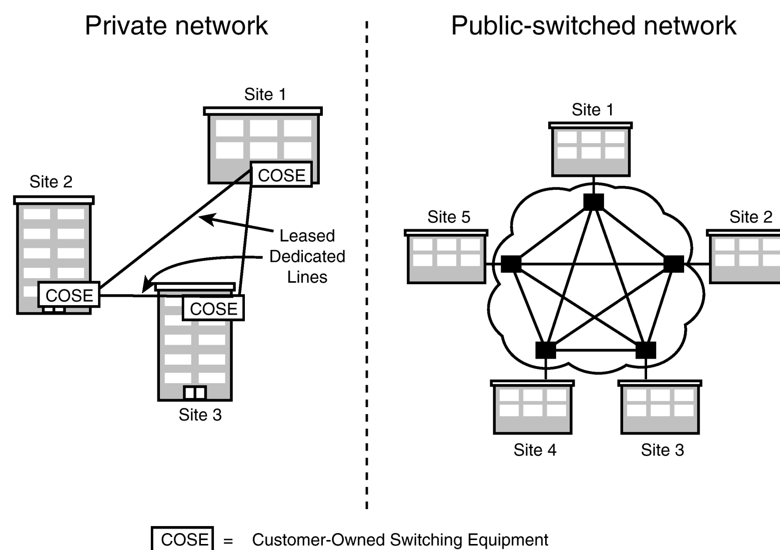
עם חיבור ייעודי יש לך גישה מלאה לכבל ואתה יכול לשלוח בו נתונים ככל שהוא יכול להכיל. אף אחד אחר אינו יכול להשתמש בקווים שחכרת.

אתה משלם **מחיר קבוע** עבור החיבור (בהתאם לסוג הקו), ללא תלות בכמות הנתונים שתעביר (או לא תעביר) בקו. קווים ייעודיים במהירויות גבוהות יקרים בדרך כלל.

רשתות ממותגות (Switched)

זהו קו ציבורי המושכר לך באופן זמני. **רשתות ממותגות** (switched networks), שלא כמו חיבור ייעודי, מאפשרות למספר משתמשים להשתתף באותו קו, אם כי לא באותו זמן. אפשרות זו ממומשת באמצעות חומרה ותוכנה הממתגות הלוך ושוב בין המקורות השונים הרוצים להשתמש בחיבור נתון.

ניתן לראות את ההבדל בתרשים 13.1. ברשת פרטית, אתה מקים חיבור, או קו, ייעודי בין כל האתרים. אתה מתחזק את כל הציוד המחבר בין האתרים ורק חוכר את הקווים עצמם מספק שירותים.



תרשים 13.1: *רשת פרטית (private network) משתמשת בקווים ייעודיים, ואילו רשת ממותגת (publick-switched network) משתמשת ברשת משותפת*

ברשת ממותגת אתה מחבר כל אתר לרשת של ספק השירותים. ספק השירותים מתחזק את כל הציוד ומקים את החיבורים בין האתרים. רשתות ממותגות מיוצגות לעיתים בדמות ענן, מכיון שהן למעשה **רשת סריג** (mesh) עם נתיבים רבים ושונים שבהם נתונים יכולים לעבור בין חיבורים.

אחת העוצמות של רשתות ממותגות היא בכך שהן יכולות לספק קישוריות "any-to-any", או במילים אחרות, לחבר בקלות כל אתר אל כל אתר אחר. אילו היית צריך להעביר ממקומו את אחד האתרים ברשת הפרטית המתוארת בתרשים 13.1, היה עליך להפסיק את פעולתה ולהתקין מחדש את כל החיבורים הייעודיים בעלות גבוהה מאוד. ברשת הממותגת, יש לכל משרד רק חיבור אחד לרשת הממותגת הגדולה יותר. העברת המשרד תהיה כרוכה בשינוי חיבור נתונים אחד בלבד.

רשתות ממותגות גם מתמודדות בקלות עם תמיכה בארגונים הגדלים וזקוקים לתעבורה רבה יותר. ככל שחברה גדלה וזקוקה לרוחב פס (bandwidth) רשת גדול יותר, ניתן לרוב להרחיב את החיבור הממותג. רשתות ממותגות אחדות אף מספקות **רוחב פס-לפי-דרישה** (bandwidth-on-demand), המאפשר לחברות להשתמש ברוחב פס רחב יותר בשעות השיא ולשלם תעריף נוסף, מעבר לתעריף החודשי הרגיל. לדוגמה, חברה יכולה לחתום חוזה עבור רשת עם רוחב פס של 128Kbps; אך היא תוכל להשתמש ברוחב שעד 256Kbps בשעת הצורך ותשלם על תוספת רוחב הפס רק כשהוא בשימוש.

התעריפים שונים ברשתות ממותגות לעומת אלה של קווים חכורים. עם קו חכור אתה משלם תעריף חודשי קבוע, ללא תלות במידת השימוש בקו. לעומת זאת, ספקי שירות ברשתות ממותגות גובים ממך תשלום התלוי ברוחב הפס של הרשת שהיה בשימוש.

קיימים שני סוגים של רשתות ממותגות:

- ✯ **מיתוג-מעגלים** (circuit switching). מספק חיבור בלעדי זמני בין שתי נקודות.
- ✯ **מיתוג-מנות** (packet switching). מספק חיבור משותף בין מספר נקודות.

מיתוג-מעגלים (Circuit)

בכל פעם שאתה מרים את הטלפון, אתה משתמש ברשת ממותגת-מעגלים. כאשר אתה מתקשר למישהו, מוקם **מעגל** (circuit) בין הטלפון שלך לבין הטלפון של אותו גורם. במשך שיחת הטלפון שלכם יש לכם גישה בלעדית לקווי הטלפון שביניכם. רק כאשר תנתקו יוכל מישהו אחר להשתמש בקווי הטלפון שבהם עברו עד כה האותות שלכם.

אם תתקשר לאותו גורם עשר פעמים באותו יום, שיחת הטלפון עשויה לעבור בדיוק באותם קווים בכל עשר הפעמים, או לעבור על פני קווי טלפון שונים. אינך יודע, וגם אינך צריך לדעת, מהו בדיוק המסלול שבו עברה השיחה מהטלפון שלך אל היעד.

כך גם בעולם המחשבים, חיבור ממותג-מעגלים (circuit-switched connection) יכול להתקיים ברשת של ספק השירותים בין כל שני מחשבים אישיים. דוגמאות שיידונו בהמשך הפרק כוללות חיבורי טלפון בחיוג (**dial-up**), **ISDN**, ובשירותי **Switched-56**.

רשתות מיתוג-מעגלים יכולות להיות חסכוניות, אך מהירותן מוגבלת.

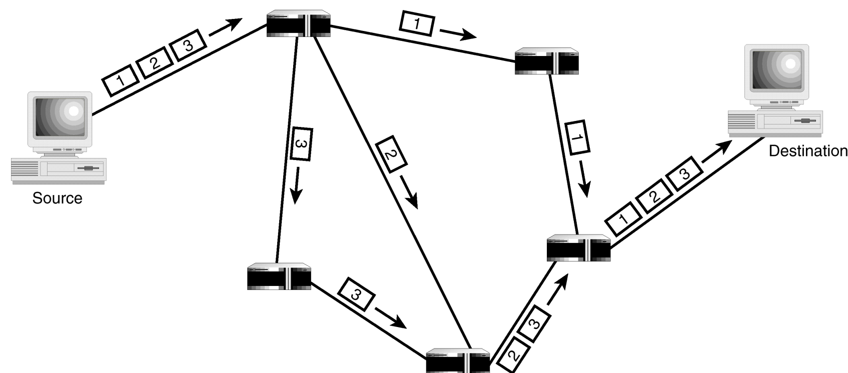
מיתוג-מנות (Packet)

כדי להבין מהו מיתוג מנות (packet switching), חשוב על המצב הבא. אתה אחראי להובלת משא עבור חברה בבוסטון; אך עליך לשלוח לסן-פרנציסקו משלוח גדול מכדי שיהיה כדאי ואפשרי להעבירו במטוס. במקום זאת, עליך לשקול הובלת משא זה ברכבת או במשאית. אם תשלח ברכבת, ייקח זמן מה לטעון את כל המשא לתוך קרונות, לחבר ביניהם ולשלח אותם לדרכם. אינך יודע בדיוק באיזה מסלול תיסע הרכבת, אולם ברור לך שכל המשא יעבור יחד. אם יהיו השהיות כלשהן בדרך, כל המשא יתעכב וכאשר יגיע, הכל יגיע יחד ובאותו זמן.

לחילופין, אם תשתמש במשאיות, תוכל לטעון כל משאית ולומר לנהגים את כתובת היעד של המשלוח בסן-פרנציסקו. כאשר כל משאית הוטענה, היא יכולה להתקדם בזמנה אל הכביש המהיר ולצאת לדרך. כל נהג משאית יחליט על הנתיב שבו הוא רוצה לנסוע והוא גם יכול לשנות את הנתיב במהלך הנסיעה. אם יש עיכובים או שיבושים בדרך, הנהג יכול לשנות את הנתיב ולעקוף את האזור החסום. נהגים אחדים עשויים לבחור נתיבים מהירים יותר מאחרים, ולכן המשאיות (המטען) עלולות להגיע ליעד בסדר שונה מזה שבו יצאו לדרך. כדי לקבל את המטען כראוי, אתה מספק לכל נהג רשימת אריזה המגדירה את מקומו של המשלוח המסוים במשלוח הכולל. כאשר מגיעות כל החבילות, הן מורכבות מחדש בסדר הנכון.

רשתות מיתוג-מנות (packet switching) דומות למשאיות, ואילו רשתות מיתוג-מעגלים (circuit switching) דומות לרכבת. ברשת מיתוג-מנות הנתונים מחולקים למנות קטנות ונשלחים לרשת. כל מנה זורמת לרשת בנפרד ומנותבת בהתאם לנתיב הטוב ביותר שנבחר ברגע כניסתה לרשת. במהלך המעבר ברשת המנה יכולה לעבור התקני חיבור שונים ורבים (connection devices, "צמתים"), וכל אחד מהם יכול לנתב את המנה לנתיב אחר.

כפי שמוצג בתרשים 13.2, התוצאה יכולה להיות מנות העוברות בנתיבים שונים ומגיעות ליעד לא לפי הסדר שבו יצאו לדרך. לכן, כל מנה מצוידת במידע סדרתי ב**כותרת המנה** (packet header), כדי שזרימת הנתונים תוכל להיות מורכבת מחדש לפי הסדר הנכון.



תרשים 13.2: ברשת ממותגת-מנות כל מנה יכולה לעבור בנתיב שונה לחלוטין בדרכה אל היעד

התעבורה ברשתות יכולה להיות **מהירה** ויעילה מאוד, מכיון שרשתות מיתוג-מנות (switched) משתמשות ב**מנות קטנות** בדרך כלל. משתמשים משלמים בדרך כלל רק עבור כמות הנתונים שהם שולחים אל הרשת, להבדיל מהתעריף הקבוע המשולם עבור קווים ייעודיים (dedicated).



רעיון מפתח

רשתות מיתוג-מנות מחלקות את הנתונים למנות קטנות הנשלחות ברשת, כך שכל מנה עוברת בנתיב הטוב ביותר האפשרי.

רשתות מיתוג-מנות אחדות יכולות לשפר ביצועים על ידי הקמת **מעגל מדומה** (virtual circuit) בין שתי נקודות ברשת. למעשה, המעגל המדומה משלב את התפישות של רשתות מיתוג-מעגלים (circuit switching) ומיתוג-מנות (packet switching). כאשר נוצר חיבור בין שתי נקודות, מוקם מעגל ברשת בין שתי הנקודות. כל מנות הנתונים עוברות באותו נתיב מהמקור אל היעד, אולם עדיין משתתפות ברשת עם מנות של משתמשים אחרים. באנלוגיית המשאיות, הדבר דומה להנחיית כל נהג משאית לנסוע בנתיב מסוים בין בוסטון לסן-פרנציסקו. המשאיות ייסעו כולן באותו נתיב, אולם הכבישים שהן עוברות בהן ישרתו גם נהגים אחרים.

מעגלים מדומים מאפשרים לרשתות להסיר מעט מתקורת ההעברה, מכיון שהתקני החיבור אינם צריכים לקבוע את הנתיב הטוב ביותר שבו תעבור מנה. המנה מגיעה בדרך כלל עם המעגל בכותרת שלה, כך שהתקן החיבור צריך רק להעביר אותה הלאה להתקן הבא במעגל.

כאשר מוקם מעגל מדומה עבור חיבור זמני בין שני התקנים, הוא נקרא **מעגל מדומה ממותג - SVC** (switched virtual circuit). כאשר חיבור זה קבוע, כמו למשל בין שני נתבים המקוונים תמיד, החיבור נקרא **מעגל מדומה קבוע - PVC** (permanent virtual circuit). מעגלי PVC משמשים ברבות מטכנולוגיות מיתוג המנות המתקדמות הזמינות כיום.



רעיון מפתח

מעגלים מדומים מקימים נתיב לתמסורת מנות ברשת מיתוג-מנות.

מיתוג תאים (cell-switching) הוא מונח המשמש את העוסקים בטכנולוגיית ATM (Asynchronous Transfer Mode, המוסברת בהמשך הפרק בסעיף "ATM"), כדי לתאר את גירסת ATM למיתוג-מנות. במיתוג-תאים, כל מנות הנתונים מחולקות ל**תאים** קטנים מאוד ("יחידות נתונים") בעלי אורך קבוע (ATM משתמשת בתא באורך 53 בתים) אשר מועברים ברשת. מכיון שכל רשתות מיתוג-מנות המסורתיות מאפשרות שינוי אורך מנת הנתונים, התקני מיתוג-מנות צריכים להיות מסוגלים לזהות את תחילת המנה ואת סופה. התקורה הכרוכה בחישובים אלה עלולה להשפיע על מהירות ביצועי הרשת.

עם מנות נתונים באורך קבוע, רשתות מיתוג-תאים יכולות לבנות את המיתוג לתוך התקני חומרה המשמשים ברשת, וכך לאפשר תמסורת מהירה יותר של נתונים.



רעיון מפתח

מיתוג-תאים (cell switching) הוא גירסה של מיתוג-מנות, שבה הנתונים מחולקים לתאים קטנים מאוד בעלי **אורך קבוע**.

טכנולוגיות WAN

קיימות מספר טכנולוגיות שונות למימוש חיבור WAN. בהמשך הפרק נדון בטכנולוגיות WAN הבאות:

1. מערכת הטלפון,
2. מיתוג מנות X.25,
3. ממסור מסגרות (Frame Relay),
4. ATM (Asynchronous Transfer Mode),
5. SMDS (Switched Multi-megabit Data Service),
6. SONET (Synchronous Optical Network).

1. מערכת הטלפון

אחד הרכיבים הבסיסיים של קישוריות WAN הוא מערכת הטלפון התקנית, שכולנו מכירים. **רשת טלפונים ציבורית ממותגת - PSTN** (Public Switched Telephone Network) קיימת למעלה ממאה שנה והיא פרושה בכל העולם. בארצות רבות מופעלת PSTN על ידי סוכנות ממשלתית, או ארגון ציבורי אחר. בארה״ב מופעלת PSTN על ידי מערכת מורכבת, הכוללת חברות טלפון מקומיות (לדוגמה, RBOCs - Regional Bell Operating Companies) ומפעילות שיחות חוץ שונות, כגון AT&T, SPRINT ו-MCI.

בעת התקנת קווי טלפון לבית או למשרד שלך, חברת הטלפון המקומית מכניסה חיבור חוט טלפון ל**נקודת תיחום** (demarcation point), שהיא לרוב תיבת סיעוף כלשהי בבניין. כמנוי לשירות הטלפון אתה אחראי להתקנה ותחזוקה של כל קווי הטלפון הפנימיים העוברים ברחבי המשרד עד לחיבורם לנקודת התיחום. למרות שתוכל להעסיק את חברת הטלפון המקומית, או חברת כבלים אחרת, להתקנת החיבורים הפנימיים, דע שהם אינם חלק מאחריות החברה.

חברת הטלפון אחראית לחיבור מנקודת התיחום אל **המשרד המרכזי - CO** (central office) הקרוב ביותר של החברה, ובפשטות - **המרכזיה של הארגון**. חיבור זה, הנקרא **מעגל מקומי** (local loop), הוא בדרך כלל כבל UTP או כבל סיב-אופטי. חברת הטלפון המקומית אחראית לכל התחזוקה, האיתות (כגון צליל החיוג וצליל תפוס) וסינון רעש עבור חיבור מקומי זה. על פני אותו חיבור, חברת הטלפון גם מספקת את המתח החשמלי הדרוש לפעולת הטלפון.

כל מרכזיה (CO) מקומית מאגדת מרכזיות נוספות באמצעות קווים בינעירוניים מהירים, כדי ליצור את הרשת הגדולה יותר של חברת הטלפון המקומית. מפעילי שיחות חוץ מחברים קווים במהירות גבוהה מרשתות החוץ שלהם אל הרשת של חברת הטלפון המקומית. חברת הטלפון המקומית מסתמכת על מפעילי שיחות החוץ לאספקת חיבורים לאזורים אחרים ומסביב לעולם.

בעת חיבור שיחות טלפון, PSTN משתמשת במיתוג-מעגלים (circuit switching). החיבור שלך בין **נקודת התיחום** (demarcation point) במשרד שלך לבין CO המקומית נעשה באמצעות כבל פיסי ייעודי. כל שיחה שתבצע, תמיד תעבור באותו כבל יחיד אל המרכזיה המקומית. אולם מרגע שהשיחות מגיעות אל המרכזיה, נוצר מעגל בנתיב המתאים ביותר לביצוע השיחה. כל המעגלים מחוברים ומנותקים במרכזיה המקומית.

עבור חיבורי הרשת המרחבית (WAN) המשתמשים ברשת טלפונים ציבורית ממותגת (PSTN), קיימים חמישה סוגים שונים של חיבורים אפשריים:

א. חיבורים בחיוג (dial-up),

ב. קווים חכורים ייעודיים (dedicated),

ג. Switched-56,

ד. T-Carrier System,

ה. ISDN (Integrated Services Digital Network).

1א. חיבורים בחיוג (dial-up)

חיבורים בחיוג על פני PSTN נפוצים מאוד כיום באמצעות קווי טלפון אנלוגיים. על ידי שימוש פשוט במודם, יכול המחשב להתחבר למחשב אחר דרך קו טלפון לא יקר.

אולם, מכיון שרשת מסוג PSTN היא ממותגת-מעגלים, איכות החיבור עשויה להשתנות בכל פעם שנוצר קשר. בנוסף, למרות שיצרני מודמים מכריזים כעת על אפשרות שידור בקצב של 56Kbps בערך, ההפרעות האלקטרומגנטיות בקווים גורמות לכך שצריך לעבוד במהירויות נמוכות יותר.

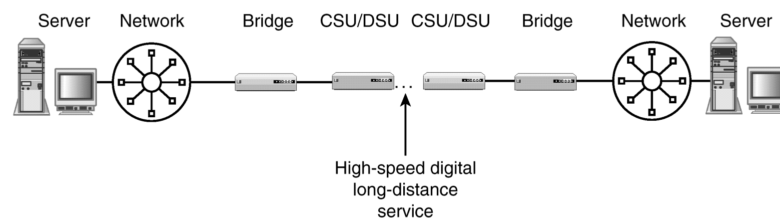
1ב. קווים חכורים ייעודיים (dedicated)

כשלב אחד מעל חיבורים בחיוג, מציעים חברות טלפון וספקי שירותים אחרים **קווים חכורים ייעודיים** (dedicated leased lines). קווים חכורים מספקים חיבור ייעודי, כל הזמן, בין שתי נקודות ב-PSTN. מכיון שחברת הטלפון מקצה קו לשימוש הבלעדי שלך, קווים חכורים עשויים להיות יקרים. כאשר הקווים אינם ממותגי-מעגלים, ניתן לבדוק את איכות הקו וגם להגדיר את הציוד הדרוש כדי לאפשר תמסורת נתונים במהירות גבוהה. אפשר לחכור קווים ייעודיים אנלוגיים, או דיגיטליים.

עבור **קווים אנלוגיים ייעודיים** חכורים משתמשים במודמים רגילים, אולם אלה סובלים ממגבלות פיסיות רבות, כמו חיבורים בחיוג. מכיון שאותות אנלוגיים רגישים מאוד **להפרעות אלקטרומגנטיות (EMI)**, יש להשתמש במנגנוני בדיקת שגיאות כדי להבטיח העברת נתונים מוצלחת. מנגנונים מסוג זה גורמים לחיבורים אנלוגיים להיות איטיים, ולא שימושיים במיוחד.

מסיבות אלו, רוב הארגונים חוכרים קווים ייעודיים דיגיטליים. **קווים דיגיטליים** מותאמים לשימוש נתונים ואינם רגישים ל-EMI באותה מידה כמו קווים אנלוגיים. קווים דיגיטליים יכולים לאפשר שידור נקי משגיאות ב-99 אחוזים. קווים ייעודיים דיגיטליים נקראים לרוב בשם **קווי DDS** (Digital Data Service), כהתייחסות לשם המקורי שניתן על ידי AT&T לשירות זה. קווי DDS מספקים חיבורי נקודה-לנקודה במהירויות 2.4, 4.8, 9.6, 19.2 או 56Kbps.

מכיון שקווי DDS הם דיגיטליים, אין צורך להשתמש במודם כדי להתחבר לקו החכור. החיבור מבוצע באמצעות התקן **CSU/DSU** (Channel Service Unit/Data Service Unit), כפי שמוצג בתרשים 13.3. חלק CSU של היחידה מתחבר לקו DDS, וחלק DSU מתחבר לרשת המקומית שלך. CSU/DSU ממיר אותות מרשת המקומית לצורך תמסורת בקו DDS, ובנוסף מספק אלקטרוניקה להגנת איכות האות בשתי הרשתות.



תרשים 13.3: *יחידות CSU/DSU משמשות לחיבור שתי רשתות על פני קו חכור*



הערה: ייתכן ותיתקל ב-DSU שיפורש כ- Digital Service Unit במקום Data Service Unit.

למרות שקווי DDS חכורים מספקים חלופה לחיבור בחיוג, העלות שלהם והמגבלה של 56Kbps גרמו לירידה בפופולריות שלהם, ככל שהתפתחו טכנולוגיות חדשות כדוגמת ממסור מסגרות (frame relay, שנדון בה בהמשך הפרק).

1ג. Switched-56

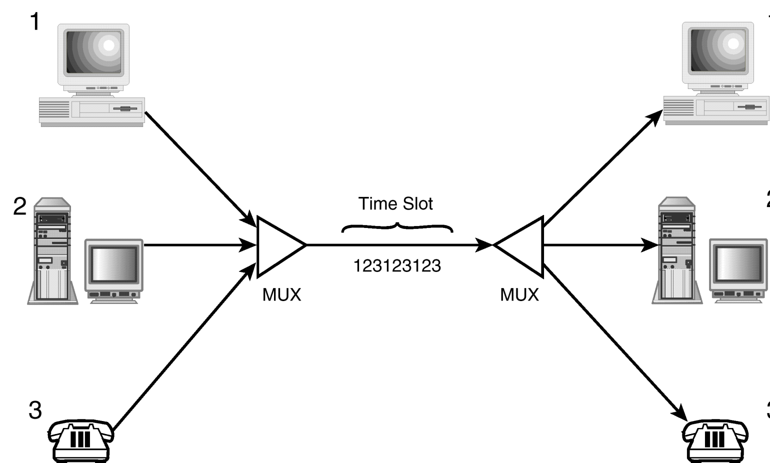
חברות וארגונים שונים רצו מהירות קו 56Kbps חכור, אולם לא רצו לשלם עבור קו בלעדי עבורם, ואז החלו חברות טלפון וספקי שירותים להציע שירות Switched-56. שירות זה אינו אלא גירסה ממותגת-מעגלים של קו DDS 56Kbps חכור. מכיון שמשתמשים משלמים רק עבור הזמן שבו הם מחוברים, העלויות הכרוכות בכך עשויות להיות נמוכות הרבה יותר מאשר עבור קו חכור.

כדי להשתמש בחיבורי Switched-56, שני קצות החיבור חייבים להיות מצוידים ב- CSU/DSU תואם Switched-56 כדי שיוכלו לחייג ולהתחבר זה לזה.

1ד. T-Carrier System

בימים הראשונים של PSTN, כל כבל טלפון יכול היה לשאת רק שיחת טלפון אחת. עם הגידול בדרישה ובשימוש בקווי טלפון, חיפשו חברות הטלפון פתרון להקלת הצפיפות של קווי קול. בשנות ה-60, פיתחו בחברת Bell (Bell Telephone Laboratories) את **T-carrier system** כדי לענות על דרישה זו. למרות שהמערכת החלה כמערכת אנלוגית באיכות קול, AT&T החלה להציע שירות T-carrier דיגיטלי בשנת 1983.

כפי שמוצג בתרשים 13.4, מערכת T-carrier משתמשת בהתקנים הנקראים **מרבבים** (multiplexors) או muxes, לשילוב מספר ערוצי נתונים להעברה בקו תקשורת. בקצה המקבל, ישנו מרבב נוסף ש**מפרק** (או demultiplexes) את מה שהתקבל ומפריד בין הערוצים.



תרשים 13.4: *מרבבים משלבים מספר ערוצי נתונים לשידור בכבל תקשורת יחיד*

היחידה הבסיסית של מערכת T-carrier היא **קו T1** (T1 line). קו זה מורכב מ-24 ערוצי 64Kbps ועל כן הוא משיג קיבולת שידור כוללת של 1.544Mbps. כל אחד מ-24 הערוצים יכול לשמש לתקשורת קול או נתונים נפרדת, או יכול להיות משולב להשגת מהירויות שידור גבוהות יותר. במינוח טלקומוניקציה, קצב השידור של 64Kbps נקרא DS-0 (Digital Signal level 0) וקו T1 מלא נקרא DS-1. טבלה 13.1 מציגה את היכולות של סוגי הקווים השונים האפשריים במערכת T-Carrier.

טבלה 13.1: *מערכות T-Carrier*

אות	מערכת התמסורת (שידור)	קצב תמסורת (שידור) (Mbps, מיליון סל״ש)	ערוצי קול	ערוצי T1
DS-0	N/A	0.064	1	N/A
DS-1	T1	1.544	24	1
DS-2	T2	6.312	96	4
DS-3	T3	44.736	672	28
DS-4	T4	274.760	4032	168



הערה: שירות T1 זמין בכל ארצות הברית, אולם אינו בהכרח קיים בארצות אחרות. בארצות אלו ייתכן וקיים שירות דומה הנקרא E1 עם מהירות תמסורת נתונים בסיסית של 2.048Mbps.

כיום, קו T-carrier הנפוץ ביותר ברשתות מרחביות הוא T1. ניתן למצוא גם קווי T3 ברשתות אלו, אולם הם אינם נפוצים כתוצאה מהעלויות הגבוהות מאוד הכרוכות בחכירתם. קווי T2 אינם מוצעים לציבור ומשמשים רק את חברות הטלפון. הן קווי T1 והן קווי T2 יכולים להשתמש בחוטי נחושת תקניים, ואילו קווי T3 ו-T4 מחייבים שימוש בכבל סיב-אופטי, או בתווך בעל מהירות שידור גבוהה, כגון שידור מיקרוגל.

מכיון שהתקנת קו חכור T-carrier עלולה להיות יקרה מאוד, ספקי שירותים מציעים ללקוחות את היכולת להשתמש בחלק מקו T-carrier באמצעות שירותים כגון Fractional T1 ו- Fractional T3. לדוגמה, Fractional T1 מאפשר לך להשתמש במספר מסוים של ערוצי 64Kbps (עד 24 ערוצים בקו T1). לדוגמה, תוכל להחליט שאתה זקוק רק לחיבור 384Kbps בין שני משרדים. במקום לשלם עבור קו T1 כולו, תוכל לבקש מספק שירותים להשתמש רק בשישה ערוצים מתוך 24 הערוצים של הקו. יתרון עבורך הוא שבמקרה ותזדקק ליותר רוחב פס, כל שיהיה עליך לעשות הוא להתקשר לספק השירותים ולבקש הקצאת ערוצים נוספים.

חיבור הרשת לקו T1 (או T-carrier אחר) דומה מאוד לחיבור לקו DDS. דרוש לך CSU/DSU תואם T1 וגשר או נתב. אם ברצונך לשתף בקו T1 תעבורת קול ונתונים, אתה זקוק למרבב שישלב את אותות הקול והנתונים. ניתן לחכור קווי T1 מחברת הטלפון המקומית, מפעילי שיחות חוץ, או ספקי שירותים אחרים ובדרך כלל תשלם תעריף חודשי קבוע. למעשה כל ספקי השירותים מתחברים לרשת של חברת הטלפון המקומית, לכן עדיין תצטרך לחכור חיבור מעגל מקומי מהמשרד אל המרכזיה (CO) הקרובה ביותר של חברת הטלפון.

1ה. ISDN

ISDN (Integrated Services Digital Network), או **רשת דיגיטלית של שירותים משולבים**, החלה כהצעה לשלב קול, נתונים ווידאו על פני קווי טלפון מנחושת, על ידי המרת אותות הטלפון מאנלוגיים לדיגיטליים. ISDN ממומשת כיום ברחבי העולם הן על כבלי נחושת והן על כבלי סיב-אופטי באמצעות שני תקנים :

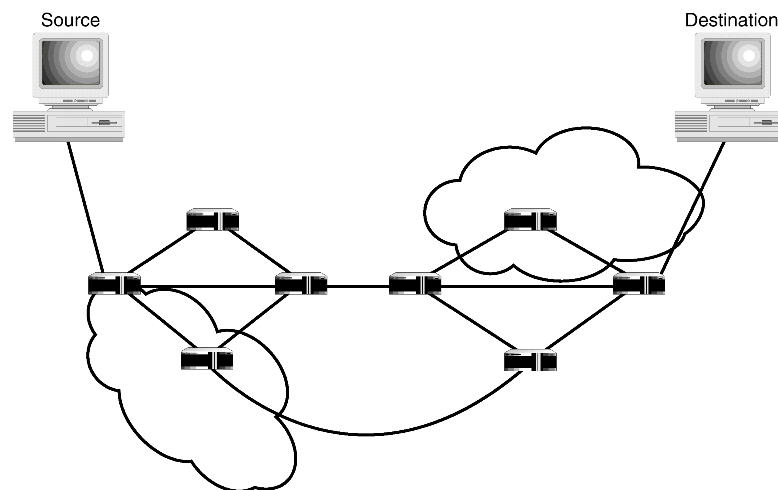
- ✭ **Basic Rate ISDN (BRI).** רשת בסיסית שמיועדת לשוק הביתי או לעסק הקטן. היא מורכבת משני ערוצי B הפועלים ב-64Kbps וערוץ D אחד הפועל ב-16Kbps. כל אחד מערוצי B יכול לשמש לקול או לנתונים, וערוץ D משמש למידע הקמת שיחה ובקרה. אחד היתרונות של BRI הוא שניתן להשתמש בערוץ B אחד לקול ובשני לנתונים, או שניתן להשתמש בשני ערוצי B משולבים כדי להשיג תמסורת במהירות שידור של 128Kbps.
- ✭ **Primary Rate ISDN (PRI).** רשת עדיפה, שמיועדת לארגונים גדולים יותר ומשתמשת בקו T1 שלם לאספקת 23 ערוצי B וערוץ D אחד. כמו ב-BRI, גם כאן ערוצי B משמשים לקול או לנתונים, וערוץ D מטפל במידע בקרה.

רשת ISDN היא שירות בחיוג שאינו מיועד לשימוש כל הזמן (full-time) כמו קו T1 ייעודי. מכיון שמשתמשים משלמים על פי השימוש בפועל ולא תעריף חודשי קבוע (כמובן, שחישוב עלות זה צריך להיות מבוסס על תעריף החיוב מחברת הבזק. בעלות של 99₪ לחיוב קו ISDN ללא קשר למספר פעימות או דקות שימוש, כדאי מאד להתשמש בקו זה ללא הפסקה), ניצול רשתות ISDN יכולים להיות כדאיים מאוד במצבים שהשימוש בהם מוגבל. ככל שעולה השימוש בקו ISDN הוא עלול להיות יקר יותר מקו חכור ייעודי רגיל. החיבור לקו ISDN מבוצע באמצעות התקן הדומה למודם (הנקרא על ידי ספקים רבים **מודם ISDN**) שאליו מתחברים המחשב ומכשיר טלפון רגיל.

2. מיתוג מנות - X.25

באמצע שנות ה-70 היו ארגונים שחיפשו חלופה לקווים חכורים ומצאו אותה ברשתות מיתוג-מנות מסוג X.25. סדרת הפרוטוקולים X.25 הוגדרה על ידי CCITT/ITU וקבעה כיצד יתחברו ההתקנים אל רשת משולבת (internetwork). בעוד שפרוטוקולי X.25 תוכננו להתאמה לכל רשת פרטית או ציבורית, הם הפכו לשם נרדף של **רשתות נתונים ציבוריות** - PDN (Public Data Networks) המשתמשות במיתוג-מנות והמופעלות על ידי חברות כגון AT&T, Tynnet ו- General Electric. רשתות PDN, שיועדו במקור לחיבור מסופים למחשבים גדולים, יכולות לספק ללקוחות חיבורים בין רשתות מקומיות בעלות נמוכה יחסית.

כפי שמוצג בתרשים 13.5, רשתות X.25 מיוצגות במקרים רבים על ידי ענן, הודות לאופי דמוי הסריג של הטופולוגיה שלהן. מנות עוברות ברשת בנתיב הטוב ביותר הזמין בכל רגע נתון.



תרשים 13.5: *רשתות X.25 משתמשות במיתוג-מנות לניתוב נתונים על פני טופולוגיית סריג*

רשתות X.25 פותחו בתקופה שבה קווי טלפון היו עדיין לא אמינים, ולכן שולבו בפרוטוקולים אלה בדיקות שגיאות רבות. כתוצאה, רשתות X.25 איטיות יחסית ויכולות להגיע למהירויות של כ-64Kbps בלבד.

חיבור הרשת המקומית לרשת X.25 כרוך בדרך כלל בחכירת קו בין הרשת המקומית לאחת הרשתות הציבוריות (PDN) הזמינות לשימוש מסחרי. החיבור לרשת המקומית יכול להתבצע באמצעות מחשב עם ממשק X.25 או דרך התקן PAD (packet assembler/disassembler).

בעוד שרשתות X.25 מספקות חיבורים מוכחים, אמינים, ללא שגיאות כמעט, השימוש בהם דועך בגלל המהירות האיטית והתפתחות טכנולוגיות כמו ממסור מסגרות ו-ATM.



רעיון מפתח

רשתות מיתוג-מנות מסוג X.25 **יכולות לספק חיבורים בעלות נמוכה לקצבי שידור עד** 64Kbps **באמצעות** PDN (Public Data Networks) **המשתרעות ברחבי העולם.**

3. ממסור מסגרות (Frame Relay)

עם התפתחות טכנולוגיית העברה דיגיטלית, קטן הצורך בבדיקת שגיאות מחמירות. טכנולוגיית **ממסור מסגרות** (frame relay) התפתחה מ-ISDN ו-X.25 על ידי הורדת תכונות בדיקת השגיאות וניהול החשבונות של X.25 ומעבר לפעול בעיקר בתווך סיב אופטי. תמסורת בשיטת ממסור מסגרות מניחה שתווך הרשת יספק איכות העברה גבוהה, ובדיקת השגיאות תהיה על ידי התקנים שנמצאים בקצות החיבור. לתמסורת ממסור מסגרות משתמשים במסגרות בעלות אורך משתנה, הפועלות בשכבת קישור הנתונים של מודל OSI.

בנוסף, בשונה ממיתוג-מנות X.25 שמשתמש בנתיב הפנוי הטוב ביותר לכל מנה, ממסור מסגרות יוצר **מעגל מדומה קבוע - PVC** (permanent virtual circuit) בין שתי נקודות ברשת. מעגל זה מגדיר נתיב דרך רשת ממסור המסגרות, ולכן הצמתים ברשת ממסור המסגרות אינם צריכים לבזבז זמן בקביעת הנתיב עבור מנת הנתונים. כתוצאה מהעדר בדיקת השגיאות ומהשימוש ב-PVC, חיבורי ממסור מסגרות יכולים לפעול במהירויות שבין 56Kbps ל- 1.544Mbps.

אחד היתרונות ללקוחות הוא שאת חיבורי ממסור מסגרות ניתן להקים עבור כל דרישת רוחב פס. כאשר אתה מבקש מספק שירותים חיבור ממסור מסגרות, החוזה הוא עבור Committed Information Rate (CIR), כלומר התחייבות לקצב שידור נתון, שיהיה קיבולת העברת הנתונים המובטחת של הקו. מציינים את קצב השידור המובטח (CIR) בדילוגים של 64Kbps. אם תחתום על CIR של 384Kbps, תובטח לך קיבולת זו. ספקי שירותים יכולים גם לספק רוחב פס גבוה יותר לפי דרישה (Bandwidth by Demand), וכך תשלם תעריף קבוע עבור ה-CIR ותשלום נוסף עבור שימוש גבוה יותר.

חיבורי ממסור מסגרות נפוצים מאוד כעת, מכיון שהם מספקים את אחד מחיבורי WAN המהירים והזולים ביותר. בעת כתיבת ספר זה, חיבור ממסור מסגרות עולה הרבה פחות מקו חכור ייעודי, או מחיבור ATM.

חיבורי ממסור מסגרות ניתן לקבל באמצעות CSU/DSU תואם ממסור מסגרות ונתב או גשר.



רעיון מפתח

רשתות ממסור מסגרות מספקות חיבור מהיר עד 1.544Mbps באמצעות מיתוג-מנות באורך משתנה על פני תווך סיב-אופטי דיגיטלי.

4. שיטת תמסורת אסינכרונית - ATM

ATM (Asynchronous Transfer Mode) היא טכנולוגיית מיתוג-מנות מתקדמת המספקת תמסורת נתונים במהירות גבוהה על פני רשתות מקומיות ורשתות מרחביות. ניתן להפעיל ATM על פני מיגוון סוגי תווך ובמערכות תמסורת פס בסיס (baseband) ופס-רחב (broadband).

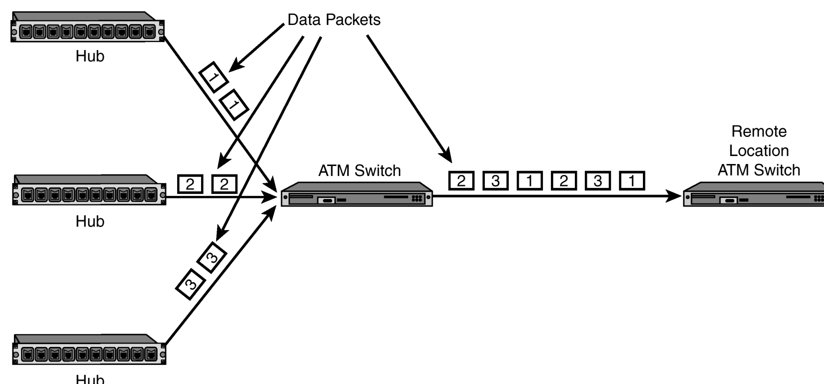
המימוש של ATM למיתוג-מנות נקרא **מיתוג-תאים** (cell-switching) מכיון שהוא משתמש במנות נתונים בעלות אורך קבוע. שלא כמו ממסור מסגרות, שבה אורך המנה יכול להשתנות, למנות ATM - הנקראות **תאים** - יש אורך קבוע של 53 בתים. מתוך 53 בתים אלה, 48 מכילים נתונים וחמישה משמשים למידע כותרת. מכיון שקל יותר לשדר מנות נתונים באורך אחיד מאשר מנות באורך אקראי, ATM מאפשרת את רוב מטלות המיתוג והניתוב באמצעות התקני חומרה. היעילות המושגת על ידי שימוש במיתוג-חומרה עם תאי נתונים קטנים מאפשרת ל-ATM להגיע למהירויות עד 622Mbps.



הערה: באופן תיאורטי ניתן להגיע למהירויות עד 1.2Gbps עם ATM, אולם כיום התמסורת בכבלי סיב-אופטי מוגבלת לרמת 622Mbps.

כמו ב-Frame Relay, גם ATM מניחה שהקו פועל ללא רעשים, ולכן היא משאירה את בדיקת השגיאות להתקני שכבת קישור הנתונים שבשני קצות החיבור. ATM גם מקימה PVC בין שתי נקודות על פני רשת ATM.

התקן החומרה העיקרי ברשת ATM הוא **מתג ATM** (ATM switch) המשמש כמרבב (multiplexor), כדי לאפשר להתקנים רבים לשדר בו-זמנית ברשת מרחבית (WAN), כפי שמוצג בתרשים 13.6. חיבור רשת מקומית שאליו מחובר המתג יכול להיות כבל קואקסיאלי או זוג שזור, אולם אף אחד מסוגי תווך אלה אינו יכול לתמוך במהירויות הגבוהות של תמסורת ATM. לכן, בדרך כלל תמצא שארכיטקטורת ATM פועלת בקווי T3 (45Mbps), ברשתות FDDI (100Mbps) או בחיבורי OC3 SONET (155Mbps).



תרשים 13.6: *מתגי ATM פועלים כמרבבים ומאפשרים תמסורת של מספר ערוצי נתונים בחיבור תקשורת יחיד*

החומרה הדרושה ל-ATM יקרה יחסית, אך למרות זאת נחשבת ATM לשיטת התמסורת העיקרית לרשתות מחשבים בעתיד. השקפה זו נובעת בעיקר מההמהירות, היעילות ויכולת הגידול של ATM מרשתות קטנות לרשתות עולמיות ומהיכולת לתפקד על מיגוון סוגי תווך.



רעיון מפתח

ATM היא טכנולוגיית מיתוג-מנות מתקדמת המעבירה נתונים בתאים בעלי אורך קבוע של 53 בתים במהירויות עד 622Mbps.

xDSL

בשלהי שנות 1990 צצו ועלו מספר גרסאות של טכנולוגיית תקשורת חדשה שנודעה בשם Digital Subscriber Loop (ובקיצור DSL). טכנולוגיה זו אפשרה למשתמשים בה חיבורים מהירים בהרבה מאלה להם היו רגילים, תוך שימוש בקווי טלפון רגילים מנחושת. הטכנולוגיה הנפוצה ביותר נהייתה טכנולוגיית ADSL (Asymmetric Digital Subscriber Loop), המאפשרת חיבור מהיר וקבוע לאינטרנט על קוי טלפון רגילים. המגבלה, כרגע, היא מרחק החיבור בין נקודת הקצה למרכזיה. למשל, במרחק של 2,700 מטר מהירות ההורדה היא 8.448Mbps ואילו במרחק של 4,800 מטר מהירות ההורדה "צונחת" ל-2.048Mbps. לזה קוראים - WOW!!!

Cable Modems

בשנים האחרונות למדנו גם על אפשרויות קישור רחב-סרט המתבסס על תשתית הטלוויזיה בכבלים. יתרונן של מערכות אלה הוא בכך שהן מאפשרות חיבור רשת קבוע אשר במערכות מסוימות אף מגיע למהירויות של רשתות מקומיות (LAN), 10Mbps.

סיכום

רשת מרחבית - WAN (Wide Area Network) מחברת מספר רשתות מקומיות (LAN) על פני מרחקים גיאוגרפיים גדולים, ומורכבת בדרך כלל מקווים בבעלותם של ספקי שירותים, קווי טלפון בחיוג (dial up), קווי טלפון חכורים (dedicated), וקווי תמסורת ברשתות מיתוג-מנות (packet switched).

קווים ייעודיים כרוכים בהקמת קו פתוח, **בלעדי וקבוע** (Full-Time) בין שתי נקודות. לעומתם, רשתות ממותגות מאפשרות למספר משתמשים להשתתף באותו קו והן יכולות להשתמש במיתוג-מעגלים (circuit switching) או מיתוג-מנות (packet switching) בעלות נמוכה בהרבה ביחס לשימוש בקווים ייעודיים.

כדי לממש רשת מרחבית, WAN, קיימות מספר טכנולוגיות שונות ובהן חיוג במערכת הטלפונים, X.25, Frame Relay, ATM, SMDS ו-SONET.

מערכת הטלפון הבסיסית יכולה לספק קווי בחיוג (dial up), קווים חכורים ייעודיים (dedicated), קווי T-carrier, או חיבורי ISDN. קווי חיוג פועלים באמצעות מודם על פני קווי טלפון אנלוגיים רגילים. קווים חכורים ייעודיים יכולים להיות אנלוגיים או דיגיטליים, וקווים חכורים DDS (dedicated Digital Service) משתמשים ב-CSU/DSU (Channel Service Unit/Data Service Unit) לחיבור הרשת לקו דיגיטלי.

מערכת T-carrier משתמשת ב**מרבבים** (multiplexors) לשילוב מספר ערוצי קול או נתונים להעברה ומורכבת מ-24 ערוצי 64Kbps למהירות העברה מירבית של 1.544Mbps.

ISDN (Integrated Services Digital Network) מאפשרת למשתמשים לשלב קול ונתונים על פני קו דיגיטלי. Primary Rate ISDN מספקת 23 ערוצי 64Kbps B וערוץ D אחד של 64Kbps, ומשתמשת ברוחב הפס המלא של קו T1.

X.25 היא סדרת פרוטוקולים של CCITT/ITU המגדירים כיצד מתרחש מיתוג-מנות (packet switching) על פני רשת משולבת. X.25 משמשת בעיקר ברשתות נתונים ציבוריות (PDN) שאליהן ארגונים יכולים להתחבר, ומספקת תקשורת אמינה, וכמעט ללא שגיאות.

ממסור מסגרות (Frame Relay) מספק מיתוג-מנות כמו X.25, אולם מניח פעולה על תווך אמין יותר ומשאיר את בדיקת השגיאות להתקנים שבקצות הקו.

ATM (Asynchronous Transfer Mode) משתמשת בצורה מתקדמת של מיתוג-מנות הנקראת מיתוג-תאים (cell switching), בה כל הנתונים ארוזים לתאים באורך 53 בתים לצורך התמסורת.

ADSL הוא האינטרנט המהיר בחיבור קבוע על קווי טלפון רגילים.

14

האינטרנט

אי אפשר לדבר על תקשורת ללא אינטרנט. ככל שתפתח את מיומנויות הרישות שלך, תיתקל בצורך לחבר את הרשת שלך לאינטרנט. פרק זה ידון ברקע של האינטרנט, וכיצד ניתן לחבר אליה את הרשת שלך.

רעיונות ונושאים עיקריים בפרק כוללים :

- סקירה כללית של האינטרנט,
- שירותים זמינים באינטרנט,
- Domain Name System,
- חיבור לאינטרנט,
- נושאי אבטחה.

ראשיתה של האינטרנט

האינטרנט העולמית - the global Internet - המקיפה של היום החלה כמערכת צנועה למדי. בשנת 1969 פיתחה **סוכנות ARPA** (Advanced Research Projects Agency) של משרד ההגנה האמריקאי רשת ניסיונית שנקראה ARPAnet לקישור ארבעה מרכזי מחשוב-על למטרות מחקר צבאי. דרישות התכנון של רשת זו היו מהירות, אמינות, וסיבולת למקרה שפצצה גרעינית תהרוס כל אחד ממרכזי המחשוב ברשת. מאותם ארבעה מחשבים מקוריים, הרשת התפתחה לרשת המשתרעת על מיליוני מחשבים שאנו מכירים כיום, רשת **האינטרנט**.

למרות שאיום הפצצה הגרעינית פחת היום, התברר שתכנון זה הינו נכס עצום לרשת תקשורת מרחבית. כל מחשב אחראי להעביר את המידע שלו למחשב אחר ולרשת עצמה אין אחריות כלשהי. אם מחשב או חיבור למחשב כושלים מסיבה כלשהי, התקשורת למחשב זה תיפסק, אולם שאר המחשבים ימשיכו לפעול ולתקשר ביניהם. הרשת לא תיפול בגלל מחשב אחד.

התרומה הגדולה ביותר אולי של ARPAnet היא פיתוח מערכת הפרוטוקולים TCP/IP. כאשר מערכת זו הפכה למערכת הפרוטוקולים התקנית ברשתות, היא אפשרה למחשבים מכל הסוגים להיות מחוברים זה לזה ולשתף מידע ביניהם.

במשך הזמן דעכה ARPAnet והוחלפה ברשת NSFnet, שגם היא הייתה במימון ממשלתי והופעלה בחסות **NSF** (National Science Foundation). גם NSFnet "סיימה את תפקידה" והוחלפה על ידי **סריג** (mesh) של רשתות מסחריות שאנו מכירים היום. ממשלת ארה"ב עדיין מממנת חלקים של האינטרנט המוקדשים לתחומים ממשלתיים, צבאיים וחינוכיים, למרות שכיום האינטרנט היא בעיקרה מפעל מסחרי.

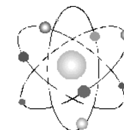
למעשה, האינטרנט עצמה היא "**רשת של רשתות**". אין כל "חברת אינטרנט" מרכזית שאליה ניתן להתחבר. לפנינו אוסף של **ספקי שירותי אינטרנט - ISP** (Internet Service Providers) המפעילים את הרשתות שלהם, עם הלקוחות שלהם, ומסכימים ביניהם להתחבר זה לזה, כדי להעביר מנות נתונים מרשת אחת לאחרת. ספקי שירותי אינטרנט גדולים רבים מוכרים לספקים קטנים יותר את אפשרות החיבור לרשת שלהם, וחלקם מוכרים חיבורים לספקי שירות אחרים.

בסופו של דבר, ספקי שירותים אלה בכל הרמות מוכרים חיבורים לבודדים ולחברות, המשלבים את הרשתות (או המחשבים הבודדים) שלהם לרשת גדולה יותר.

למרות שאין שליטה מרכזית של האינטרנט, קיימים תקני תקשורת ויש תיאום בין ספקי השירותים. הדבר נעשה בפיקוח ארגון מלכ"ר (מוסד ללא כוונת רווח) הנקרא Internet Society. ארגון נוסף כזה הוא **IETF** (Internet Engineering Task Force), שמתאם את הפעולות של מספר ועדות המגדירות תקני תקשורת אינטרנט וחוקרות שיטות להרחבה ושיפור תקשורת אינטרנט. תקני התקשורת מכונים RFC (בקשות להערות - Request for Comments) וכל ספקי השירותים נצמדים אליהם מתוך בחירה.



הערה: מבנה האינטרנט דומה לזה של רשת טלפונים. אם תחשוב על כך, כאשר אתה מתקשר למישהו, השיחה עוברת מחברת הטלפון המקומית אל מפעיל שיחות חוץ, ומשם לחברת הטלפונים של האדם שאליו אתה מתקשר, ושם נוצר החיבור הסופי. יכול אף להיות מפעיל שירותי טלפון נוסף בדרך, כמו בשיחות בינלאומיות, למשל. כל חברות הטלפון המקומיות וחברות המפעילות שירותי שיחות חוץ מסכימות לחבר בין המערכות שלהן. אינך יודע בדיוק כיצד השיחה מגיעה אל היעד - אתה רק יודע שהיא הגיעה!



גלו ה- Web

אם אתה מעוניין ללמוד עוד אודות ההיסטוריה והמבנה של האינטרנט, בקר בדפי הבית של Internet Society בכתובת

http://www.isoc.org/

ושל Internet Engineering Task Force בכתובת

http://www.ietf.org/

שירותי האינטרנט

לאחר חיבורך לאינטרנט, יש לך גישה למיגוון שירותים. להלן רשימה חלקית של השירותים הבולטים:

- גלישה באמצעות דפדפן,
- דואר אלקטרוני - E-mail,
- שרתי FTP (File Transfer Protocol),
- צ'יט (Chat),
- קבוצות דיון (Newsgroups),
- Telnet,

שירותים חדשים מוצעים כמעט מדי יום, ועם התפתחות הטכנולוגיה הם מאפשרים שימוש רב יותר באודיו (קול) ווידאו (סרטים). מספר השירותים רק ימשיך ויגדל. כל השירותים פועלים בעיקר בשכבת היישום (Application) של מודל ייחוס OSI.

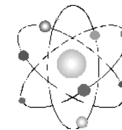
גלישה באמצעות דפדפן

World Wide Web, ובקצרה **WWW**, החל בשנת 1989 כאמצעי לפרסום מאמרי מחקר אקדמיים כדי שמדענים ברחבי העולם יוכלו לעיין בהם. מכיון שהתוכנה ששימשה הן לתצוגה והן לפרסום המידע הופצה לכל דורש, החלו משתמשים ברחבי העולם ליצור את מה שכונה מאוחר יותר בשם **אתרי Web** (Web sites). כיום, ה-Web הפך לאמצעי העיקרי לגישה למידע באינטרנט. אלפי אתרי Web חדשים מפרסמים מידע מדי יום.

מבנה ה-Web פשוט למדי. כאשר אתה רוצה לפרסם מידע שאנשים אחרים יוכלו לראות, הקבצים שלך צריכים להיות זמינים לאחרים באמצעות **שרת Web** (Web server). המסמכים, הנקראים גם **דפי Web** (Web pages), כתובים בעיקר ב-HTML (HyperText Markup Language) ויכולים לכלול מלל, גרפיקה, קול ווידאו. מדפי ה-Web שלך אתה יכול ליצור **hypertext links** (קישורים) אל דפים שנכתבו על ידי אנשים אחרים ונמצאים בשרתי Web אחרים. אתרים אחרים, במיוחד ספריות וכלי חיפוש, יוכלו ליצור גם הם **קישור** (link) אל האתר שלך, כדי שמשתמשים הפונים אליהם יוכלו למצוא את הדפים שלך. קישורים אלה בין אתרי Web יוצרים **סריג** (mesh), או **רשת עולמית** הדומה לרשת של קורי עכביש.



הערה: מיקרוסופט כוללת שרת Web במערכת Windows NT/2000, כך שתוכל להתחיל לפרסם חומר באינטרנט מייד. ב- Windows NT/2000, שרת Web הוא IIS - Internet Information Server לעבודה מאומצת. במערכת הפעלה Windows 98 הוא נקרא PWS - Personal Web Server וב- Windows NT Workstation 4.0, שרת Web נקרא Peer Web Services ומיועד לשימוש קל. מעבר לשני שרתים אלה מבית מיקרוסופט, קיימים כיום שרתי Web כמעט לכל סוג מחשב.



על ה- Web

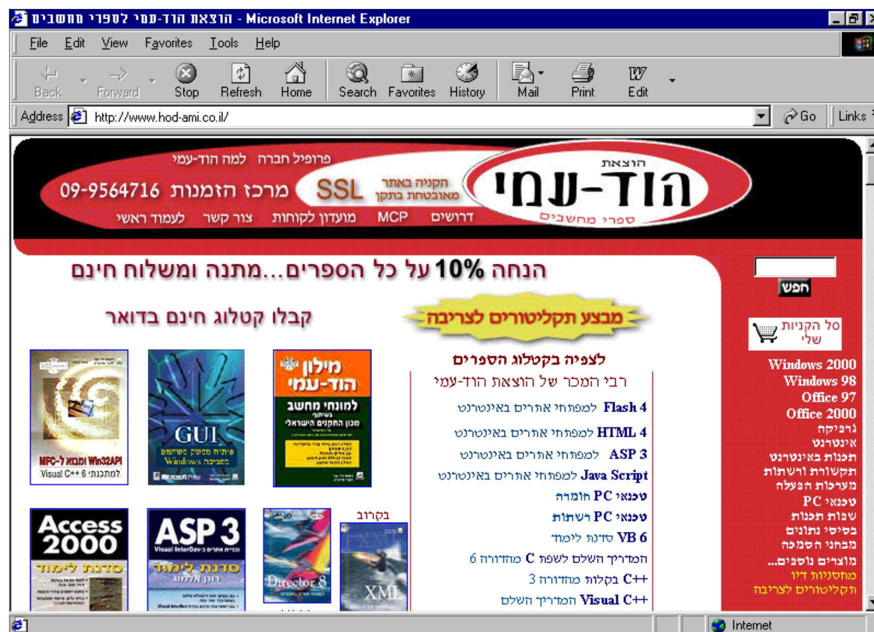
מכיון שמיקרוסופט משפרת בהתמדה את מוצר Internet Information Server שלה, כדאי לבקר באתר Web בכתובת

http://www.microsoft.com/iis/

ולוודא שבידך הגירסה העדכנית ביותר, כמו גם המידע העדכני.

משתמשים מחפשים מידע ב-Web וגם מעיינים בו באמצעות תוכנת גלישה ברשת הקרויה **דפדפן** (browser). תוכנה זו מאפשרת למשתמשים לציין לאיזה שרת Web הם רוצים להתחבר. בדרך כלל, הדפדפן מספק גם סדרת מצביעים למשתמשים שאינם בטוחים היכן הם רוצים להתחיל לחפש.

שני הדפדפנים הנפוצים ביותר הם Navigator של Netscape ו-Internet Explorer של מיקרוסופט (ראה תרשים 14.1). שניהם מאפשרים למשתמשים לראות גרפיקה ברזולוציה גבוהה, להשתמש בקול ווידאו, להציג דפי Web בעלי מבנה דף מורכב ולחפש בקלות אתרי Web חדשים.



תרשים 14.1: *ניתן להשתמש ב- Internet Explorer של מיקרוסופט להצגת אתרי Web כגון אתר הוצאת הוד-עמי בכתובת http://www.hod-ami.co.il*



הערה: Internet Explorer של מיקרוסופט נכלל חינם בכל מערכת הפעלה של Microsoft. כמו כן, תוכל למצוא אותו בכל תקליטור של הוצאת הוד-עמי, כולל תקליטור המצורף לספר זה.

דפדפני הרשת מתקשרים עם שרתי Web השונים באמצעות **פרוטוקול HTTP** (HyperText Transfer Protocol). כל האינטראקציה (יחסי הגומלין) בין הדפדפן לבין השרת מסתכמת בבקשה פשוטה לקבלת מסמך. לאחר שהשרת שולח את המסמך אל הדפדפן, אין עוד קשר כלשהו ביניהם. הדפדפן אינו צריך להתנתק (log out) משרת Web, או לציין בדרך כלשהי שסיים להשתמש בשרת. אין, ולא דרוש כל קשר (אלא אם המשתמש מבקש מסמך נוסף מהשרת).



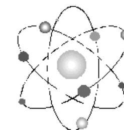
טיפ: בין כל ראשי התיבות המשמשים לפרוטוקולי רשת, זכור ש-HTTP משמש רק עבור World Wide Web.

הצלחת ה-Web והזמינות הגבוהה של דפדפני הרשת הפכה את טכנולוגיות Web לאמצעי פרסום עיקרי באינטרנט. עסקים וארגונים רבים פיתחו רשתות **אינטראנט** (intranet), שבהן שרתי Web משמשים לפרסום מידע ברשת מקומית, או רשת מרחבית ארגונית. לדוגמה, ספרי הדרכה פנימיים, מידע של מחלקת משאבי אנוש ומדיניות חברה ניתן להפיץ באמצעות שרת Web באינטראנט, במקום להדפיס ולחלק אותם בצורה מודפסת.



רעיון מפתח

כאשר אנשים מדברים על פיתוח אינטראנט, הם מתכוונים **לשימוש בטכנולוגיות אינטרנט ברשת פנימית של הארגון. ככלל, שרתי Web ברשת פנימית זו אינם זמינים למשתמשים ברשת האינטרנט החיצונית.**



על ה- Web

אם אתה רוצה ללמוד את כל הפיתוחים העדכניים בנושא World Wide Web, בקר בדף הבית של קונסורציום World Wide Web בכתובת http://www.w3.org/

דואר אלקטרוני

דואר אלקטרוני (electronic mail) או **e-mail**, הוא הסיבה העיקרית שלשמה אנשים מתחברים (או מחברים ארגון) לאינטרנט. World Wide Web הוא האמצעי העיקרי שבו אנשים משתמשים לאיתור ולאחזור מידע, והדבר מרגש, מעניין ומסעיר ללא כל ספק. עם זאת, הדואר האלקטרוני הוא "סוס העבודה" של האינטרנט, השומר על קיום התקשורת.

כדי להשתמש בדואר אלקטרוני, המשתמש זקוק לתוכנת **לקוח** (client) של דואר אלקטרוני. תוכנה זו יכולה להיות ייעודית לדואר אינטרנט (למשל, Eudora), או שהיא יכולה להיות תוכנת דואר אלקטרוני שהיא חלק מתוכנה מקיפה, כמו Microsoft Exchange, Microsoft Mail, או Lotus cc:Mail שיש לה **שער** (gateway) אל האינטרנט.

משתמשים שולחים הודעה זה לזה ומשתמשים בכתובות בסגנון אינטרנט, שנראות כך: user@domain. בכתובת זו, user הוא שם המשתמש המוקצה לו על ידי ספק השירותים (ISP), ו-domain הוא הכתובת עצמה כדוגמת hod-ami.co.il שמות **תחומים** (domains) כוללים לרוב את שם החברה או שם הארגון, ולאחריו ציון התחום ברמה העליונה, בן שלושה תווים (ראה סעיף "The Domain Name System" בהמשך הפרק למידע נוסף אודות שמות תחומים וההבדלים בין השמות בארה"ב ובארצות אחרות). לדוגמה, כדי לתקשר עם הוצאת הוד-עמי, תוכל לשלוח דואר אלקטרוני לכתובת info@hod-ami.co.il.

הודעות דואר אלקטרוני נשלחות דרך האינטרנט באמצעות רשת של **שרתי דואר** (mail servers) האחראים לאספקה וקבלה של דואר אלקטרוני. שרתים אלה משתמשים בעיקר ב**פרוטוקול SMTP** (Simple Mail Transfer Protocol) לשיגור וקבלת דואר אלקטרוני. דואר אלקטרוני המיועד למשתמש שהמחשב שלו **אינו מקוון** (offline) באותו רגע יכול להישמר בשרת, והמשתמש יוכל "למשוך" או לאחזר אותו מאוחר יותר באמצעות **פרוטוקול POP3** (Post Office Protocol 3). פרוטוקולים אלה פועלים בשכבת היישום (Application) של מודל OSI.



טיפ: נזכיר שוב, אל תתבלבל בעניין פרוטוקולי רשת. זכור ש-SMTP ו-POP3 הם פרוטוקולים למשלוח וקבלת דואר אלקטרוני באינטרנט, ואינם פרוטוקולי שידור ברשת.

שרתי FTP (File Transfer Protocol)

ב-Web תמצא כמויות גדולות של נתונים שרובם טקסט או גרפיקה. כשתרצה להוריד קבצי נתונים גדולים המכילים תוכנה או נתונים אחרים, תצטרך להשתמש ב**פרוטוקול העברת הקבצים - FTP** (File Transfer Protocol). בגלל השימוש הרב בו, פרוטוקול FTP נכלל כמעט תמיד בכל התקנה של מערכת הפרוטוקולים TCP/IP. ומסיבה זו תראה שמרבית ספקי התוכנה מאפשרים גישה לתוכנות שלהם באמצעות שרת FTP. למשתמש המחובר לאינטרנט לא תהיה בהכרח דפדפן, אולם קרוב לוודאי שותקנה אצלו תוכנת לקוח FTP.

לקוחות FTP זמינים בשתי צורות: **מבוסס טקסט** (text based), ומבוסס **גרפיקה** (graphical). לקוחות FTP מבוססי טקסט החלו בעולם UNIX ולכן הם שומרים על מבנה הפקודות הקצרות ממערכת UNIX. מחלון טקסט, כמו שורת פקודה (ראה תרשים 14.2), ניתן לכתוב את הפקודה **ftp**, להתחבר למארח המפעיל שרת FTP, ולהתחיל להוריד קבצים.

```
ftp> open ftp.microsoft.com
Connected to ftp.microsoft.com.
220 ftp Microsoft FTP Service (Version 2.0).
User (ftp.microsoft.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-This is FTP.MICROSOFT.COM.  Please see the
 dirmap.txt file for more information.
230 Anonymous user logged in.
ftp> ls dirmap.txt
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
dirmap.txt
226 Transfer complete.
12 bytes received in 0.01 seconds (1.20 Kbytes/sec)
ftp> get dirmap.txt
```

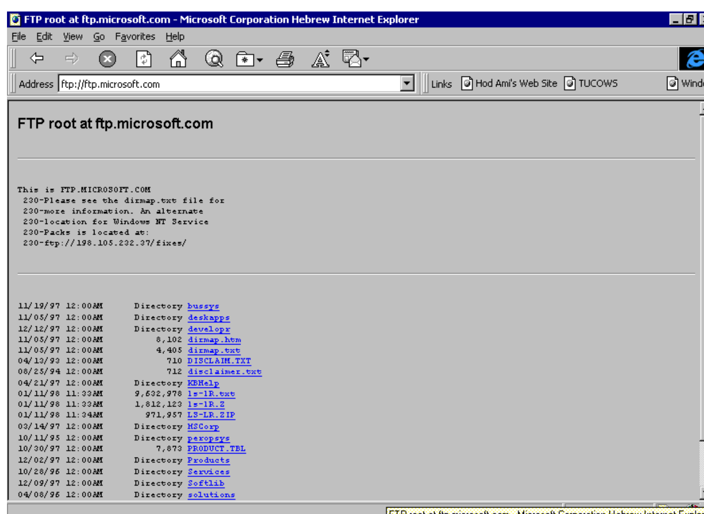
תרשים 14.2: *לקוח FTP מבוסס טקסט מסופק עם מערכות הפעלה רבות*



הערה: לקוח FTP מבוסס טקסט נכלל הן ב-Windows 95 והן ב-Windows NT בעת התקנת TCP/IP.

לקוחות FTP גרפיים זמינים בצורות רבות. קיימות תוכניות מיוחדות המיועדות לספק גישת FTP באמצעות ממשק גרפי. אולם לרוב תראה אנשים המשתמשים בדפדפני רשת להורדת קבצים. הן Internet Explorer של מיקרוסופט והן Netscape Navigator, כמו גם דפדפנים אחרים, תומכים בהורדת קבצים באמצעות FTP, כפי שמוצג בתרשים 14.3.

בגלל קלות אחזור הקבצים באמצעות הדפדפנים, משתמשים רבים ב-Web ימשיכו להוריד קבצים (כלומר, להעתיק אותם אל המחשב שלהם), בלי להיות מודעים כלל לכך שלעיתים הם משתמשים ב-FTP.



תרשים 14.3: *דפדפן Internet Explorer של מיקרוסופט יכול לשמש להורדת קבצים באמצעות FTP*



הערה: Internet Information Server של מיקרוסופט, שכלול במערכת Windows NT 4.0, פועל כשרת Web, אולם יכול גם לפעול כשרת FTP.

Chat

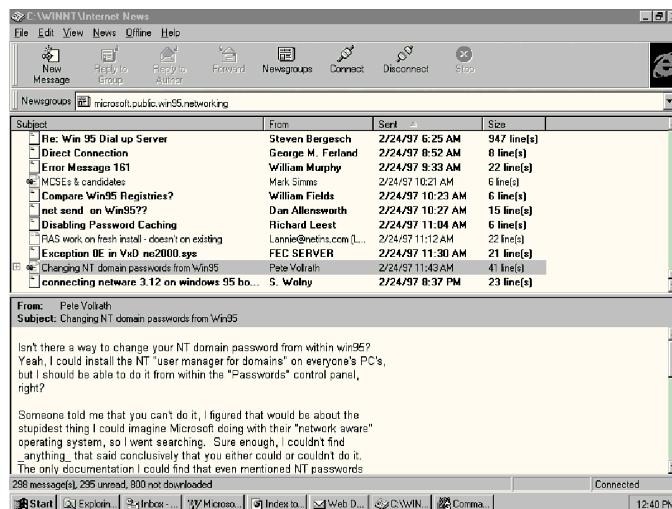
רבים ממשתמשי האינטרנט "מצ'טצ'טים" ביניהם באמצעות תוכנות לקוח כגון ICQ או IRC. CHAT הוא קישור ישיר בזמן-אמת בין משתמשים המחוברים באותו זמן לאינטרנט. תוכנות CHAT רבות מאפשרות גם קישור וידאו וקול, במידה ורוחב הפס מאפשר זאת. למרות זאת, הקישור הטקסטואלי הוא עדיין הקישור הסטנדרטי.

קבוצות דיון (Newsgroups)

בתחילת התפתחות האינטרנט נעשה מאמץ מקביל לפתח רשת המחברת בין מחשבים לקיום קבוצות דיון. רשת זו, המכונה UseNet, התפתחה לסדרת **קבוצות דיון** (newsgroups) ששותפו בין מחשבים באמצעות **פרוטוקול NNTP** (Network News Transport Protocol). עם הזמן, קבוצות דיון אלו החלו לעבור באינטרנט, וכעת הן נחשבות חלק משירותי האינטרנט.

כיום יש עשרות אלפי קבוצות דיון שונות הדנות כמעט בכל נושא שניתן להעלות על הדעת. ממערכות הפעלה לספורט, פוליטיקה, דת, בידור ועוד. אלפי מאמרים נשלחים לקבוצות דיון ברחבי העולם בכל דקה במשך היום.

כל המערכת פועלת באמצעות סדרה של **שרתי דיון** (news servers) המופעלים בדרך כלל על ידי ספקי שירותי אינטרנט, אוניברסיטאות, או חברות. כל שרת דיון עוסק במספר קבוצות דיון המשותפות למשתמשים בשירותיו. כאשר אתה **שולח** (post) מאמר לקבוצת דיון, הוא זמין בשרת הדיון של ספק שירותי האינטרנט שלך. בתוך דקות עד שעות, המאמר יופץ לכל שרתי הדיון בעולם העוסקים בקבוצת דיון זו. בדרך זו מתרחש דיון כלל עולמי בנושא כלשהו.



תרשים 14.4: *ניתן להשתמש ב- Internet News של מיקרוסופט לקריאת קבוצת דיון*

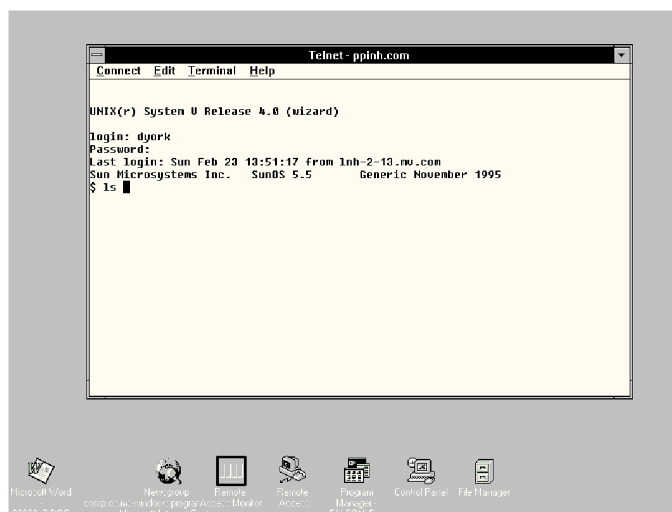
ניתן להשתתף בקבוצות דיון באמצעות תוכנית לקוח הנקראת **news reader**, כפי שמוצג בתרשים 14.4. אבל המגמה היא לאפשר ביצוע של כל הפעולות באינטרנט דרך הדפדפן, כמו Internet Explorer או Netscape Navigator.



הערה: חברות רבות התקינו שרתי דיון באינטראנט שלהן, כדי לספק פורומים מקוונים (online) לעובדי הארגון לדיון בנושאים המעסיקים אותם בתוך הארגון.

Telnet

בימים הראשונים של האינטרנט, מחשבים מהירים היו יקרים ונדירים מאוד. למעשה, רשת ARPAnet המקורית נוצרה לשיתוף מחשבי-על בין חוקרים רבים. אחד הצרכים הנפוצים ביותר היה שחוקרים במקום אחד יתחברו למחשבי-על מרוחקים אלה לביצוע מחקריהם עתירי החישובים. לצורך זה פותחה תוכנית Telnet. באמצעות הפקודה telnet, ניתן להתחבר למחשב מארח רחוק ולתקשר איתו כאילו היית מחובר אליו ישירות, כפי שמוצג בתרשים 14.5. המארח המרוחק צריך להריץ Telnet server (הנקרא בדרך כלל Telnet daemon או Telnetd) ולאפשר למספר משתמשים להתקשר בו-זמנית.



תרשים 14.5: *הפקודה telnet מאפשרת להתחבר למארח מרוחק*



הערה: Windows 95 ו-Windows NT מתקינים לקוח Telnet עם התקנת TCP/IP. קיים שרת Telnet ל- Windows NT Server כחלק מ- Windows NT 4.0 Resource Kit.

The Domain Name System

בפרק 8 "פרוטוקולי רשת", למדת על TCP/IP וכיצד מחשבים מתקשרים באמצעות כתובות IP בעלות מבנה מספרי, כגון 192.168.10.123. למרות ששיטה זו מתאימה למחשבים, לאנשים יש קושי רב לזכור את כל המספרים האלה ודוגמתם. אם מישהו היה אומר לך "לקבלת מידע נוסף אודות החברה שלנו, בקר באתר Web בכתובת http://207.22.13.4", קרוב לוודאי שהיית מחייך אליו בנימוס ושוכח את הכתובת.

כדי להתמודד עם הצורך לזכור כתובות, פיתחה קהילת האינטרנט את **מערכת שמות התחום** - Domain Name System, המוכרת בשם **DNS**. במערכת זו, מוקצה לכל ארגון **שם תחום** (domain name), כגון **microsoft.com** או productivitypoint.com, המזהה באופן ייחודי את הארגון ברחבי האינטרנט.



רעיון מפתח

שם תחום (domain name) ב-DNS שונה מאוד מה**תחום** המוכר לנו ב-Windows NT. **שם תחום** DNS מזהה את הארגון שלך בפני משתמשי אינטרנט אחרים. אם אתה שולח ומקבל דואר אלקטרוני, או מפרסם מידע ב-Web, שם תחום DNS שלך ישולב בכתובת הדואר האלקטרוני שלך, או בכתובת שרת Web. **תחום** (domain) ברשת Windows NT Server הוא קבוצת מחשבים המשתמשים באבטחה ברמת המשתמש.

בכל פעם שאתה מתקשר ברשת לכתובת כגון **www.microsoft.com**, המחשב שלך מציג שאילתה **לשרת DNS** (DNS server) מקומי (הנקרא גם name server) כדי לברר את כתובת IP של www.microsoft.com. כאשר שרת DNS מחזיר את כתובת IP המתאימה, המחשב שלך שולח את מנות הנתונים אל כתובת זו. כל התקשורת בין מחשבים באינטרנט מבוססת על שימוש בכתובות IP. אם מסיבה כלשהי שרת DNS שלך אינו יכול למצוא את כתובת IP עבור שם התחום שהקלדת, לא תיווצר תקשורת ותקבל הודעה על כך.



הערה: DNS משתמשת בהיררכיה שלמה של שרתי DNS מבוזרים לפענוח כתובות. אם שרת DNS המקומי יודע את כתובת IP של www.microsoft.com, הוא שולח אותה חזרה למחשב. אם לא, הוא מעביר את הבקשה אל שרתי DNS ברמה גבוהה יותר, כדי לדעת איזה שרת DNS אחראי על microsoft.com. כלומר, שרת DNS המקומי מתקשר עם שרת DNS מרוחק זה כדי לברר את כתובת IP של www.microsoft.com, מחזיר את כתובת IP אל המחשב שלך ומאחסן אותה במחשב המקומי למקרה שאתה (או אחרים ברשת המקומית) תרצה לבקר באתר זה שוב.

שמות תחומים מחולקים למספר תחומים ברמה עליונה (top-level domains), כפי שמוצג בטבלה 14.1. לארגונים וחברות שנמצאים מחוץ למדינות ארה"ב, יש בדרך כלל קוד נוסף לציון המדינה. קוד המדינה הוא בן שתי אותיות.



הערה: למרות שקיימת האפשרות להשתמש ב-us כקוד מדינה עבור ארה"ב, מרבית הארגונים בתוך ארה"ב משתמשים באחד התחומים בני שלוש האותיות בלבד. האינטרנט נבנתה בעיקר על ידי ארגונים וסוכנויות אמריקאים והם אשר הגדירו ומשתמשים בקודי תחום בני שלוש האותיות. עם התרחבות האינטרנט לארצות אחרות, קוד המדינה בן שתי האותיות נכנס לשימוש. בארצות אחדות נעשה שימוש בתחומים של ארה"ב בתוך תחום הארץ שלהן, לדוגמה com.au. או edu.au. באוסטרליה (שים לב, הנקודה שמשמאל שייכת לשם התחום!).

טבלה 14.1: *DNS Top-Level Domains*

תחום	תיאור
.com	(commercial) ארגונים מסחריים.
.edu	(education) מוסדות חינוך, כגון מכללות ארבע שנים ואוניברסיטאות.
.gov	(government) סוכנויות ממשל, בעיקר הממשל הפדרלי של ארה"ב.
.mil	(military) ארגוניםצבאיים ואתרים צבאיים של ארה"ב.
.net	(network) ספקי שירותי אינטרנט וארגונים אחרים הקשורים לרשתות (שים לב שספקי שירותים אחדים משתמשים גם ב-com.).
.org	(organization) ארגונים שלא למטרת רווח ואחרים, שאינם מתאימים לקטגוריות אחרות.
.int	(international) ארגונים בינלאומיים.
.xx	קודי מדינה בני שתי אותיות המציינים את מיקום הארגון (לדוגמה, il עבור ישראל, fr. עבור צרפת, au. עבור אוסטרליה).

הקצאת שמות תחומים עבור ארה"ב ורוב מדינות העולם מטופלת כיום על ידי הארגון InterNIC. הארגון מקצה גם כתובות IP, והוא מופעל על ידי חברה פרטית על פי חוזה עם ממשל ארה"ב. הדבר ישתנה ככל הנראה בשנים הקרובות, מכיון שקיים מאמץ להוסיף TLD נוספים ולאפשר לארגונים אחרים מלבד InterNIC לרשום שמות תחומים.

למעשה, כדי לקבל שם תחום, אתה קובע איזה תחום ברמה העליונה מתאים לארגון שלך, ואז מנסה למצוא שם שאינו בשימוש על ידי מישהו אחר. זהו המאבק האמיתי של עולם DNS, אשר גרר אין ספור תביעות משפטיות הקשורות בסימנים מסחריים, זכויות יוצרים, וכדי. מכיון שיכול להיות שם ייחודי **אחד** בשם תחום, ארגונים בתחומי תעשייה שונים עם שמות או ראשי תיבות דומים, אינם יכולים להשתמש באותו שם תחום.



הערה: הבעיה של שם משתמש יחיד בכל אחד מהמספר המוגבל של שמות תחומים השפיע על אחד מנותני החסות לספר זה, Productivity Point International, שרצה להשתמש בשם ppi.com. אולם שם זה כבר נתפש על ידי חברת תרופות (שגם ראשי התיבות שלה הם PPI) כאשר Productivity Point International רצתה להתחבר לאינטרנט, Productivity Point נאלצה לקבל את שמות התחומים propoint.com ו- productivitypoint.com.

לאחר קבלת שם תחום, אתה או ספק השירותים שלך חייבים להפעיל שרת DNS שיענה על בקשות מאתרי אינטרנט אחרים לקבלת מידע אודות התחום שלך. אתה אחראי להקמת שמות כגון www.yourcompany.domain וקישור, או הצבעה שלהם אל כתובות IP תקפות.



רעיון מפתח

DNS (Domain Name System) היא מערכת המתרגמת **שמות תחומים** (domain names) לכתובות IP, ומאפשרת לאנשים להתקשר עם שירותי אינטרנט כמו ה-Web באמצעות שמות טקסט במקום מספרים.



הערה: Microsoft Windows NT/2000 כולל שרת DNS שבו תוכל להשתמש ברשת שלך.

חיבור אל האינטרנט

תהליך חיבור הרשת שלך לאינטרנט כרוך במספר שלבים:

- קביעת ספק השירותים (ISP) שישמש לחיבור,
- קבלת תחום תקף של כתובות IP מספק השירותים,
- המרת הרשת שלך לשימוש ב-TCP/IP עם הכתובות החדשות,
- התקנת החומרה המתאימה והפעלת החיבור.

בחירת ספק שירותי האינטרנט - ISP

בחירת ספק שירותי האינטרנט הינה החלטה חשובה. ספקי שירותי אינטרנט עשויים להיות חברות תקשורת גדולות, או ארגונים קטנים. הם מספקים מיגוון שירותים, אפשרויות ומחירים.

שאלות חשובות שיש לשאול ספק שירותים אפשרי הן:

- **תמיכה טכנית** (technical support). לא חשוב מה יאמרו אנשי השיווק, אף חיבור LAN לאינטרנט אינו פשוט כמו חיבור הרשת לתקע טלפון בקיר. איזה סוג תמיכה מוצעת על ידי ספק השירות עבור ההתקנה? האם הוא ישלח מישהו שיעזור? האם יש מרכז תמיכה - שנקרא לעיתים **NIC** (Network Information Center) או **NOC** (Network Operations Center) - והאם הוא מאויש במשרה מלאה? האם מישהו זמין 24 שעות ביממה, שבעה ימים בשבוע?
- **יתירות** (redundancy). כיצד מחובר הספק אל ספקי שירותים אחרים? האם יש רק קו אחד המחבר אותו אל ספק גדול יותר? האם יש מספר קווים? כיצד הוא מאורגן במקרה של **נפילות** (outages)?

* **קירבה לאפיק השידרה** (proximity to the backbone). ספקי השירותים הגדולים ביותר מפעילים **אפיקי שידרה** (backbones) עולמיים בעצמם, המורכבים מקווי תקשורת במהירות גבוהה מאוד. רוב ספקי השירותים האחרים קונים חיבורים מספקי שירותים גדולים אלה. עד כמה קרוב הספק שלך לאפיק השידרה? האם הוא חוכר קווים ישירות מאחד הספקים הגדולים? האם הוא מרוחק מספר חיבורים מאפיק השידרה? אם אתה מחפש רק חיבור לדואר אלקטרוני, ההבדל לא יהיה משמעותי. אם בכוונתך להשתמש הרבה ב-Web, כקורא או כמפרסם, המרחק מאפיקי השידרה עלול להוות הבדל משמעותי במונחים של מהירות הגישה לשירותי האינטרנט. אולם דע שהמחיר בדרך כלל עולה במידה משמעותית עם הקרבה לאפיקי השדרה.
* **אבטחה** (security). איזו הגנה מוצעת? ספקים אחדים יקימו עבורך **קיר מגן** (firewall), אחרים יפקחו על האתר שלך, ויהיו שימכרו לך רק חיבור.
* **שירותים** (services). איזה שירותים מוצעים? האם יארחו (ישמרו) עבורך דפי Web? האם יפעילו שרת דואר? האם יספקו גישה לקבוצות דיון?
* **כתובות IP** (IP addresses). כמה כתובות IP יכול ספק שירותי האינטרנט לספק לך? האם הוא יכול להקצות מספיק כתובות עבור כל המחשבים שלך? או האם הוא יכול לספק רק כתובות מעטות?
* **שמות תחומים ו-DNS** (domain names and DNS). האם ספק שירותי האינטרנט ישיג **שם תחום** (domain name, שנסביר בהרחבה בהמשך הפרק) עבורך? האם יפעיל שרת שמות DNS שיתמוך בתחום זה?
* **ציוד חיבור** (connection equipment). האם ספק השירותים יספק את ציוד החיבור הדרוש (נתבים, CSU/DSU) עבורך? האם הוא יחכיר לך את הציוד? האם ידרוש שתקנה אותו? אם כן, האם הוא יכול להציע מחיר טוב?

עליך להחליט איזה סוג חיבור אתה צריך. האם חיבור האינטרנט יהיה מרכיב קריטי בתשתית התקשורת שלך ובמערך המחשוב? האם אתה זקוק להבטחת פעילות בכל עת? האם תסתמך הרבה על החיבור לשיווק ומכירות? או האם החיבור יהיה כלי מחקר ופיתוח? האם רק מספר אנשים בארגון ישתמשו בו? או שיהיה זמין במקום העבודה עבור כולם?

יהיה עליך להתייחס לכל השאלות האלו לפני שתוכל לבצע בחירה נכונה של ספק שירותי אינטרנט עבור הארגון שלך.

קבלת תחום כתובות IP תקף מספק השירותים

כאשר אתה משתמש במערכת פרוטוקול TCP/IP ברשת הפנימית שלך (Lan), אתה יכול להשתמש בכל תחום של כתובות IP. אך ברגע שתחבר את הרשת לאינטרנט, עליך להשתמש בתחום כתובות IP ייחודי, שאף אחד אחר בכל רחבי האינטרנט אינו משתמש בו.

חשוב על כך במונחי מערכת הטלפון, שבה כל מספר טלפון הינו ייחודי. כאשר אתה מחייג בארה״ב 603-471-0848, אתה מגיע לטלפון מסוים בארה״ב, אך כשאתה מחוץ לארה״ב עליך להוסיף למספר זה את קידומת המדינה. שילוב קידומות מדינות ומספרי טלפון ייחודי במדינה מספק לך ״כתובת״ ייחודית לכל מספר טלפון בעולם. אם המערכת לא היתה פועלת כך, השיחות לא היו עוברות.

כך גם בעולם האינטרנט, לכל מחשב צריכה להיות **כתובת IP ייחודית**. בדומה למספר טלפון, כתובת זו תזהה את המחשב שלך בפני שאר העולם בעת שתשתמש באינטרנט.

לאחר בחירת ספק שירותים, עליך לקבל ממנו תחום כתובות IP עבור המחשבים ברשת שלך. רוב ספקי השירותים קיבלו הקצאה של תחום כתובות מ-InterNIC, הארגון האחראי היום על הקצאת כתובות IP ושמות תחומים. כאשר תקבל את תחום הכתובות, עליך להבטיח שכל המחשבים בארגון שלך שייגשו לאינטרנט ישתמשו בפרוטוקול TCP/IP עם כתובות חדשות אלו. אם לא תשתמש בכתובות תקפות, המחשבים שלך לא יוכלו לתקשר עם אתרי אינטרנט אחרים.

ספק השירותים גם יכול לפעול יחד איתך לקבלת שם תחום (domain name) תקף עבור הארגון שלך. שם זה, כמו למשל microsoft.com, יזהה אותך בפני העולם הן עבור כתובות דואר אלקטרוני והן עבור מאמצי הפרסום באינטרנט (אתרי Web, שרתי FTP, וכדי). כפי שהוזכר בסעיף הקודם, מישהו (אתה או ספק השירותים שלך) יצטרך לספק שירות שם DNS עבור שם תחום זה. בסיום מטלות אלו תוכל להמשיך.

הפעלת החיבור

לסיום, הפעלת החיבור לאינטרנט אינה שונה ממה שתואר בפרק 13, ״רשתות מרחביות (WANs)״. חיבור לאינטרנט אינו אלא חיבור TCP/IP WAN בין הרשת שלך לבין הרשת של ספק השירותים שלך. תצטרך להשתמש בציוד הדרוש (בדרך כלל נתב (router) ויחידות CSU/DSU), לבקש מחברת הטלפון המקומית להתקין חיבור מקומי, ולבקש מספק השירותים (ISP) להפעיל את החיבור אליך.



הערה: כאשר ספק השירותים מפעיל את החיבור שלך לאינטרנט, אתה חייב להשתמש בכתובות IP תקפות, אחרת לא תוכל לתקשר עם אתרים אחרים באינטרנט.

אבטחה והאינטרנט

אבטחה באינטרנט היא נושא שיכול בקלות למלא מספר ספרים. קיימים נושאים מסוימים שיש להתייחס אליהם לפני החיבור לאינטרנט. לאחר החיבור אל ספק שירותי האינטרנט, מנות TCP/IP שלך יכולות לזרום ממך אל אתרים בכל מקום באינטרנט העולמית. באופן דומה, מנות TCP/IP מאתרי אינטרנט אחרים יוכלו לזרום אל הרשת **שלך**.

עם הכנה ותכנון זהירים, ניתן להפחית את האיום על הרשת שלך, אולם **לא** ניתן להסירו לחלוטין. בין אם בשביל ה"כיף" ובין אם למטרות ריגול תעשייתי, משתמשים אחדים באינטרנט מוצאים כל העת דרכים חדשות להיכנס למערכות אחרות. הרשת היחידה המובטחת לחלוטין מפני חדירות מהאינטרנט, היא רשת ש**אינה** מחוברת לאינטרנט.

קיר מגן FireWall

מחסומים המגינים עליך מפני חדירות נקראים **קירות מגן** (Firewalls). **קיר מגן** הוא בדרך כלל סדרת התקני חומרה ותוכנה המגבילים את הגישה לרשת שלך. קירות מגן אחדים ניתן לממש באמצעות התקני חומרה בלבד; אחרים עשויים להיות מבוססים בעיקר על תוכנה. הטובים שביניהם משלבים מרכיבי חומרה ותוכנה גם יחד.

קירות מגן אופייניים מכילים מספר מרכיבים. חלקם כל כך נפוצים עד שראוי לאזכר אותם כאן.

הצפנה באמצעות מפתח ציבורי ופרטי

שיטת ההצפנה החדישה ביותר במחשבים היא גישת **מפתח ציבורי (Public Key) ומפתח פרטי (Private Key)**.

בעיה שתמיד ליוותה הצפנות היא העברת מפתח הקוד או הצופן לנמען שקיבל את ההודעה המוצפנת. שיטה הידועה **כמפתח ציבורי ומפתח פרטי דורשת** מהשולח והנמען להיות בעלי מפתחות.

הנמען יוצר שני מפתחות: מפתח ציבורי ומפתח פרטי. מערכת מפתח ציבורי מבוססת-מחשב משתמשת בתוכנה המצפינה נתונים בהסתמך על המפתח הציבורי של **הנמען** (ולא של השולח). קוד המפתח הציבורי ידוע לכל, והוא משמש כמדריך לפענוח הודעות (ידוע גם כצופן, או סוג ההצפנה המשמשת).

המפתח הציבורי נוצר על ידי תוכנת ההצפנה והוא שונה עבור כל משתמש. את המפתח הציבורי שולח הנמען לכל מי שמעוניין להעביר לו מסר. לאחר שההודעה הוצפנה ונשלחה לנמען, רק הנמען יכול לפענחה, באמצעות המפתח הפרטי שלו.

על שני הצדדים להיות בעלי תוכנת ההצפנה. אם אדם א׳ רוצה לשלוח הודעה מוצפנת לאדם ב׳, הוא קודם ישיג את המפתח הציבורי של ב׳.

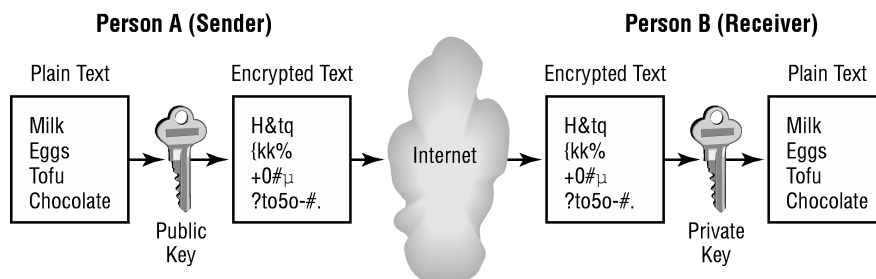
וכך זה מתנהל:

לירן רוצה לשלוח מסר מוצפן לשרון, לשם כך היא זקוקה למפתח הציבורי של שרון (נניח ששרון שולחת לה את המפתח הציבורי שלה בדואר אלקטרוני או מאפשרת לה להוריד את המפתח הציבורי מהאתר שלה). בעזרת המפתח הציבורי של שרון, לירן מצפינה את ההודעה ושולחת אותה לשרון (נניח בדואר אלקטרוני). שרון מקבלת את ההודעה המוצפנת ומכיון שבידה (ורק בידה) ישנו המפתח הפרטי התואם את המפתח הציבורי שבעזרתו הוצפנה ההודעה, המשמעות היא שרק היא תוכל לקרוא את תוכנה.

כך, המפתח הפרטי בשילוב עם תוכנת הפענוח משמשת לפענוח הודעה שהוצפנה באמצעות המפתח הצבורי של המשתמש ואותה תוכנת הצפנה. ללא המפתח הפרטי לפענוח הקובץ המוצפן, הקובץ חסר משמעות.

שיטה זו עובדת במיוחד טוב עבור אדם הצריך לקבל הודעות דואר אלקטרוני מוצפנות מאנשים רבים. כל השולחים יכולים להשתמש בתוכנת המפתח הציבורי להצפנת הודעות, אך רק הנמען יכול לפענח אותם.

תרשים 14.6 מתאר את ההליך כולו.

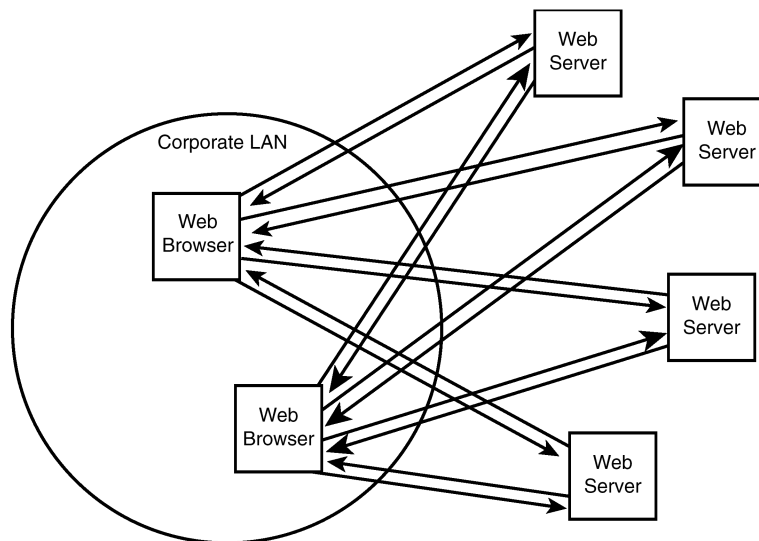


תרשים 14.6: *הצפנה ופענוח באמצעות מפתח ציבורי*

בנוסף להצפנת קבצים, שיטת המפתח הציבורי יכולה לשמש כאמצעי אימות של הודעות או קבצי נתונים אחרים כדי לוודא שהם אכן הגיעו מהשולח.

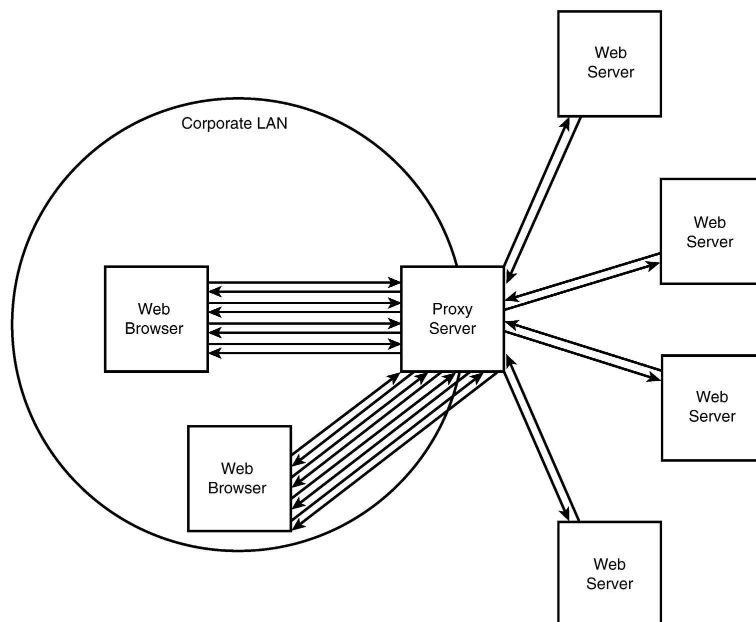
שרתים מורשים (Proxy Servers)

כאשר אתה מתקשר באינטרנט אל שרת Web, שרת זה מקליט מידע מסוים אודות הביקור שלך, כגון כתובת IP של המחשב שלך, סוג תוכנת הגלישה שבה אתה משתמש ומועד הביקור. כפי שניתן לראות בתרשים 14.7, כאשר משתמשים בארגון שלך מבקרים בשרתי Web, אותם שרתים צוברים נתוני כתובות של הארגון שלך. משתמשים מתוחכמים יכולים לנסות להשתמש בכתובות אלו כדי לחדור לרשת שלך.



תרשים 14.7: *ללא שרת מורשה (proxy server), כל המשתמשים מתקשרים ישירות עם אתרי Web*

שרת מורשה (proxy server) הוא תוכנה המפחיתה איום חדירה זה. עם התקנתו, כאשר משתמש מבקש לאחזר דף מה-Web, הדפדפן יצור קשר עם שרת proxy, אשר יאחזר עבורו את המנה ויעביר אותה אליו. כפי שניתן לראות בתרשים 14.8, התוצאה היא ששרתי Web באינטרנט ירשמו רק את הכתובת של שרת proxy, והם לא ידעו את הכתובות הפרטניות של המחשבים המבקשים את הדפים. שרת מורשה פועל בדרך כלל במחשב המוגן על ידי תוכנת קיר מגן (Firewall) כלשהי, כדי להקשות על חדירות.



תרשים 14.8: *עם שרת מורשה (proxy server), כל המשתמשים מתקשרים לאתרי Web על ידי מעבר דרך השרת*

שרתים מורשים גם משמשים לרישום מידע אודות אתרי Web שבהם ביקרו המשתמשים שלך, בנוסף להגבלת הגישה לאתרים מסוימים. שרתים אלה יכולים לשמור בזיכרון מטמון על דיסק מקומי את הדפים המבוקשים לעיתים קרובות, כדי שבקשות בעתיד ייענו במהירות.

סיכום

האינטרנט של היום, שהחלה במחקר צבאי בתקופת המלחמה הקרה הפכה לאמצעי תקשורת עולמי. למעשה זוהי רשת תקשורת מרחבית ענקית בפרוטוקול TCP/IP המורכבת מרשתות רבות של ספקי שירותי אינטרנט המחוברות ביניהן. לאחר התחברות לאינטרנט, יש לך גישה למספר גדול של שירותים ובהם World Wide Web, דואר אלקטרוני, FTP וקבוצות דיון.

כל התקשורת באינטרנט מתרחשת בין מחשבים המשתמשים בכתובות **IP**. אולם כדי לסייע למשתמשים לזכור כתובות פותחה **מערכת שמות תחומים** - **DNS** (Domain Name System). DNS מאפשרת לנו לקשר **שם תחום** (domain name) עם כתובת IP ולהשתמש בשמות בעלי משמעות לצורכי התקשרות.

כדי להתחבר לאינטרנט, עליך לדאוג לחיבור באמצעות **ספק שירותי אינטרנט - ISP** (Internet Service Provider). קיימים סוגים רבים של ספקי שירותים, והבחירה עבור הארגון שלך חשובה מאוד. לאחר בחירת ISP, עליך לקבל תחום כתובות IP תקף ושם תחום.

לפני הפעלה סופית של החיבור לאינטרנט, עליך לבחון את נושאי האבטחה ולהגדיר סוג כלשהו של **קיר מגן** (Firewall) להגנת הרשת שלך מפני חדירות לא רצויות ולהשתמש במפתח ציבורי ופרטי להצפנת המידע.

15

ניהול רשת

שים לב: המידע בפרק זה מתרכז במערכת Windows NT אבל ברובו הוא ישים גם לגבי Windows 2000 מכיון ששתי המערכות בנויות על אותה הטכנולוגיה.

לאחר התקנה והגדרה של החומרה והתוכנה עבור הרשת, אחריות **מנהל הרשת** (network administration), או **מינהלן רשת**, אינה מסתיימת. בפרק זה, תלמד עוד אודות תחומי האחריות של מנהל רשת. כשתגיע לסוף פרק זה, תוכל:

- לתאר את המשימות הבסיסיות של מנהל רשת,
- להסביר את ההבדלים בין תחום Windows NT לבין קבוצת עבודה,
- להבין את הנושאים הכרוכים ביצירת משתמשים וקבוצות ברשת,
- לזהות בעיות אבטחת רשת ושיטות לפתרון בעיות אלו.

ניהול רשת (Administering a Network)

התקנה והגדרה ראשונית של הרשת הן רק תחילת עבודתך ברשת. במהלך עבודתך יהיו עדכונים שוטפים לרשת כשתוסיף משתמשים חדשים; יהיה צורך להגדיר ולשתף מדפסות חדשות; כונני דיסק על שרתי קבצים יתמלאו וידרשו ארגון מחדש; מחשבים יפלו ויהיה צורך לשחזר נתונים; יתפתחו צווארי בקבוק ברשת; משתמשים יעזבו את הארגון ויהיה צורך להסיר את חשבונותיהם.

מנהלי רשת אחראים לניהול הרשת ופתרון בעיות מסוג זה. כמנהל רשת, תהיה אחראי על שמירת פעולה תקינה של הרשת (כאשר הרשת תיכשל או תיפול מסיבה כלשהי, נחש מי יקבל שיחות טלפון כועסות?).

כאשר אתה משמש כמנהל רשת, תחומי האחריות שלך ניתנים להגדרה כללית:

- ✯ יצירת משאבי רשת,
- ✯ ניהול משאבי רשת קיימים,
- ✯ אבטחת הרשת מפני גישה לא מורשית,
- ✯ הגנת הרשת מפני תקלות,
- ✯ תחזוקת הרשת.

בראשית ספר זה למדת את הבסיס לניהול משאבי רשת, כגון שיתוף קבצים ומדפסות. פרק זה דן ביצירה וניהול של **חשבונות משתמשים** (user accounts). תלמד גם אודות אבטחת רשת וכיצד להקצות הרשאות גישה למשאבי רשת.

ראשית, עליך להבין את ההקשר שבו תבצע את ניהול הרשת. ברשתות מיקרוסופט תעבוד במסגרת **תחום** (domain), או במסגרת **קבוצת עבודה** (workgroup). הכלים שבהם תשתמש שונים מעט, לפי סביבת העבודה.

תחומים וקבוצות עבודה (Domains and Workgroups)

תחום או קבוצת עבודה מספקים מנגנון לאיחוד לוגי של קבוצת מחשבים. לדוגמה, תאר לעצמך 200 מחשבים ברשת, בזמן שקבוצת המכירות מונה עשרה מחשבים בלבד. אם כל המחשבים נמצאים בקבוצה גדולה אחת, בכל פעם שאחד מנציגי המכירות ירצה לגשת לנתונים ממחשב אחר במחלקת המכירות, עליו לדפדף ברשימה ארוכה של 200 מחשבים למציאת המחשב המסוים הדרוש לו.

כדי לפתור בעיה זו ניתן לארגן את עשרת המחשבים של מחלקת המכירות לקבוצת עבודה, או תחום, שייקרא SALES. כעת, כאשר נציג המכירות ירצה לגשת למידע הנמצא במחשב אחר, הוא יראה תחילה רק את המחשבים בקבוצת העבודה או תחום SALES. אם נציג המכירות ירצה לגשת למחשב שמחוץ לקבוצת המכירות, הוא יוכל לעשות זאת, אך הדבר יהיה כרוך בצעד נוסף של חיפוש בקבוצת עבודה או בתחום אחר.

ברשת מקומית פיסית אחת יכולים להתקיים מספר קבוצות עבודה או תחומים. לדוגמה, יכולות להיות לך קבוצות עבודה או תחומים כגון SALES, MARKETING, RESEARCH, IS, ACCOUNTING ו-TRAINING. כל תחום או קבוצת עבודה מספקים הקבצה לוגית של מחשבים, וכל אחד יכול לספק את האבטחה שלו. כאשר אתה מחבר את המחשב שלך לרשת, תוכל לבחור בין חיבור המחשב לקבוצת עבודה (Workgroup)

או לתחום (Domain), כפי שמוצג בתרשים 15.1. מחשב אינו יכול להיות חבר במספר קבוצות עבודה או תחומים בעת ובעונה אחת, וגם אינו יכול להיות חבר (member) בקבוצת עבודה ובתחום באותו זמן. מחשב יכול להיות חבר בקבוצה לוגית אחת בלבד.



תרשים 15.1: *מאפיין הרשת, Network Properties של Windows 95 מאפשר למשתמש להצטרף לתחום או לקבוצת עבודה באמצעות תיבת הדו-שיח Network*

באשר להבדל בין קבוצות עבודה לתחומים, עליך להיזכר בקיומן של רשתות **שוויוניות** (peer-to-peer) ורשתות **מבוססות שרת** (server based). ברשתות המשתמשות במערכות הפעלה של מיקרוסופט, למימוש **קבוצת עבודה** (workgroup) משתמשים ברישות שוויוני, ולמימוש **תחום** (domain) משתמשים ברישות מבוסס שרת.

ב**קבוצת עבודה**, כל מחשב אחראי לתחזוקת רשימת משתמשים והגדרות האבטחה עבור עצמו. כשנוספים משתמשים, צריך לרשום אותם בבסיס נתוני החשבונות שבכל מחשב ברשת. אם אתה עובד עם מספר מחשבים שונים, עליך להגדיר לעצמך חשבון בכל אחד מהם.



הערה: שים לב שהגדרות האבטחה של קבוצת העבודה משתנות בהתאם למערכת ההפעלה. ב-Windows NT תיצור חשבון משתמש מקומי עבור כל משתמש. לעומת זאת, ב-Windows 95 אינך יוצר חשבון משתמש, אלא פרופיל משתמש (user profile) העוקב אחר העדפות ממשק המשתמש.

ההבדל הוא שחשבונות משתמשים ב-Windows NT יכול ליצור רק בעל הרשאות ניהול ולכן יש בהם רמת אבטחה גבוהה, ואילו פרופילי משתמש של Windows 95 יכול ליצור כל אחד שיושב ליד מחשב Windows 95. אם משתמש לא התחבר בעבר למחשב Windows 95, הוא יכול להכניס שם משתמש וסיסמה בחלון הכניסה וכך ייווצר פרופיל משתמש חדש. בעזרת הסדר זה, Windows 95 למעשה אינה מספקת כל אבטחה, כי כל אחד יכול להיכנס לכל מחשב Windows 95.

כאשר ברצונך לגשת למידע הנמצא במחשב מרוחק בקבוצת העבודה (Workgroup), המשתמש במחשב האחר חייב להרשות לך לעשות זאת. הרשאה זו יכולה לבוא בצורת בקשת סיסמה (Windows 9x) או הגדרת הרשאה הכוללת את שם המשתמש שלך (WindowsNT). ניתן להתקין מחשבי שרת בקבוצת עבודה, אולם גם אלה צריכים לנהל לעצמם את האבטחה והרשאות הגישה.

מצד שני, **תחומים** (domains) מתממשים באמצעות Windows NT Server והם מספקים מנגנון **מבוסס-שרת** (server based) לבקרה מרכזית על חשבונות משתמשים והרשאות גישה. מחשב Windows NT Server, נקרא **בקר תחום ראשי - PDC** (Primary Domain Controller), מכיל מאגר מרכזי של כל מידע המשתמשים. כאשר משתמש רוצה להיכנס למחשב, שם המשתמש שלו נבדק ברשימת המשתמשים המרכזית שבבקר PDC. לאחר כניסה לרשת, כל הבקשות למשאבי רשת נבדקות גם הן ברשימת המשתמשים המרכזית.



הערה: בקר התחום הראשי, **PDC**, מתחזק את רשימת המשתמשים וההרשאות המרכזית וניתן לתמוך בו באמצעות מחשב אחד (או יותר), המהווה **בקר תחום גיבוי - BDC** (Backup Domain Controller). בקר תחום הגיבוי BDC מספק את אותן פעולות כמו בקר התחום הראשי PDC, ובאפשרותו לאמת משתמשים כאשר בקר התחום הראשי עסוק מדי, או כשהמחשב אינו תקין. במערכת Windows 2000 יש רק סוג אחד של בקרים הנקראים **DC**.

בקבוצת עבודה (Workgroup) מוסיפים כל משתמש לכל מחשב בנפרד, ובתחום (Domain) מוסיפים כל משתמש לרשימת המשתמשים המרכזית של PDC. לאחר ההוספה, שם המשתמש זמין לשימוש במחשבים שבכל התחום (בהנחה שלמשתמש יש הרשאה להשתמש במחשב המסוים). כאשר משתמשים (users) בתחום משתפים תיקיות או מדפסות, ההרשאות מוקצות למשתמשים ולקבוצות (groups) בתחום, ולא למשתמשים שנוצרו מקומית, כמו בקבוצות עבודה.



הערה: בדיון אודות תחומים, תשמע על מושג יצירת אמון בין תחומים (trusts relationship). נאמנות (trust) הוא קשר, או יחס, בין שני תחומים שבו תחום אחד מאפשר למשתמשים מתחום אחר גישה למשאבים שלו. במערכת Windows 2000 הדברים שונים. אמנם המושג Trust Relationship נשאר אך המשמעות שונה. השוני בקצרה: ב-Windows NT יחסי האמון הם חד-כיווניים ואילו ב-Windows 2000 היחסים הם דו-כיווניים והשאר בספר **Windows 2000 Server הכנה למבחן הסמכה**, הוצאת הוד-עמי.

אם כך, באיזה מודל עלינו להשתמש? קבוצות עבודה (Workgroup) מתאימות לסביבות עבודה קטנות (שבהן עשרה מחשבים או פחות), שבהן נושאי אבטחה אינם הבעיה העיקרית וצוות התמיכה מוגבל. אולם, מכיון שכמות הניהול גדלה כאשר משתמשים נוספים רוצים לגשת למשאבי הרשת, תחום (Domain) הוא הבחירה הטבעית עבור רשתות גדולות יותר, כתוצאה מהגידול בהיקף הניהול המרכזי.

יצירת משתמשים וקבוצות (Users Accounts and Groups)

במערכת הפעלה לרשת (NOS) מזוהים המשתמשים על ידי שם משתמש, ובמקרים רבים עליהם להזין סיסמה כדי שתאופשר להם גישה למשאבי הרשת. בנוסף, חשבונות משתמשים יכולים להיות משויכים לחשבונות קבוצה (group accounts), כדי שיוקצו להם הרשאות גישה מרוכזות.

חשבונות משתמש (Users Accounts)

חשבונות משתמש במערכת הפעלת רשת (network operating system) נוצרים, או מוגדרים בדרך כלל על ידי מנהל הרשת. מנהל הרשת יכול להגדיר את הנתונים הבאים עבור חשבון משתמש :

- user name (שם משתמש). בדרך כלל שם קצר המשמש לכניסה למערכת.
- password (סיסמה). מילה הכוללת שילוב אותיות, מספרים ותווים.
- full name (שם מלא). שם המוצג ברשימות משתמשים.
- description (תיאור). תיאור תפקיד המשתמש בארגון (למשל הדרכה, או מכירות).
- home directory (ספריית בית). ספריית ברירת מחדל לשמירת קבצים.
- login scripts (תסריטי פקודות לכניסה). קבצים אלה מופעלים בכל פעם שהמשתמש נכנס למערכת (לדוגמה, ליצירת חיבורים אל משאבי רשת).

תיאור מפורט להגדרת אפשרויות אלו על ידי מנהל הרשת והסבר מתי האפשרויות השונות זמינות, קשורים במערכת הפעלת הרשת שמשתמשים בה. מערכות הפעלה אחדות, כגון Windows NT, גם מאפשרות למנהל להגדיר מתי מותר למשתמש להיכנס ומתי החשבון ייסגר ולא ניתן יהיה להשתמש בו (לשימוש עם עובדים זמניים).

ברוב מערכות ההפעלה כיום, חשבונות משתמשים מוגדרים בעזרת ממשק גרפי כלשהו, מלבד מספר חשבונות מיוחדים המובנים מראש במחשב.

חשבונות משתמש מיוחדים

בדרך כלל, בכל מערכת הפעלת רשת קיים חשבון משתמש המזוהה כ**מנהל** (administrator) למחשב מסוים. חשבון זה נקרא **Administrator** ב-Windows NT, **Supervisor** ב- Novell NetWare, ו-**root** ברוב מערכות הפעלה UNIX. במקרים רבים, חשבון וסיסמה אלה מוגדרים בעת התקנת מערכת ההפעלה במחשב. במערכות הפעלה רבות יש להשתמש בחשבון זה להגדרת חשבונות המשתמשים הראשונים במחשב. חשבון המנהל יכול גם להקצות "**זכויות ניהול**" (administrative privileges) לחשבונות משתמשים אחרים.

חשבון מיוחד נוסף שנוצר כברירת מחדל הוא **חשבון אורח** (guest account), אשר נקרא במקרים רבים בשם **Guest**. הוא מאפשר למשתמשים להיכנס למחשב ללא סיסמה, או עם סיסמה פשוטה. בדרך כלל למשתמשים אורחים יש גישה מוגבלת אל משאבי המחשב. שים לב שב- Windows NT Server 4.0, חשבון האורח אינו פעיל (disable) כברירת מחדל (ב- Windows NT 3.51 חשבון האורח פעיל כברירת מחדל).

הוספת חשבונות משתמש

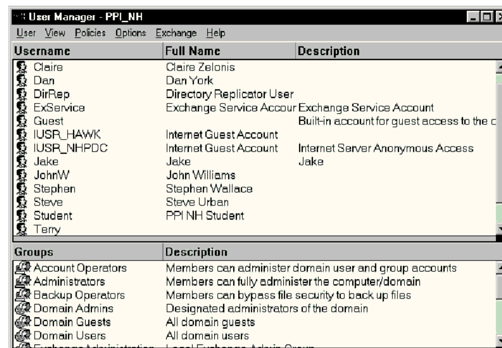
במערכות הפעלה של מיקרוסופט קיימים שני מנגנונים להוספת משתמשים למחשב. Windows 9x מספקות שיטה לא בטוחה להוספת משתמשים, ואילו Windows NT משתמשת בשיטה בטוחה יותר.

ב- Windows 95, חשבון משתמש מוגדר לראשונה שמשתמש זה נכנס למחשב. לאחר שהמשתמש מזין שם משתמש וסיסמה הוא מתבקש לאשר אותה, ואז חשבון המשתמש מוגדר במחשב. בשלב זה של התהליך לא ניתן להזין מידע נוסף אודות המשתמש, כמו למשל תיאור.

אם מחשב Windows 95 מוגדר כחלק מתחום (domain), חשבון המשתמש והסיסמה יאומתו (authenticated) על ידי **בקר תחום** (domain controller). אם הם **מאומתים** (verified) כנכונים, תהיה למשתמש גישה מלאה למשאבים מקומיים ולמשאבי רשת. אם הבחינה והאימות נכשלים, המשתמש לא יוכל לגשת למשאבי רשת מרוחקים, אולם הוא **כן** יוכל לגשת למשאבים במחשב המקומי.

לעומת זאת, חשבון משתמש במחשב Windows NT חייב להיות מוגדר לפני שהמשתמש מנסה להיכנס למערכת. כאשר משתמש נכנס למחשב Windows NT, מידע החשבון מאומת בבסיס נתוני החשבונות המקומי או בבסיס נתוני החשבונות של בקר התחום (אם המחשב הוא חלק מתחום). חשבון המשתמש חייב להימצא בבסיס הנתונים, אחרת הוא לא יוכל להשתמש במחשב (גם לא המקומי).

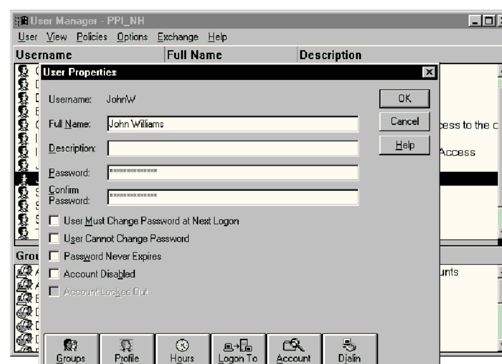
הוספת משתמשים למחשב Windows NT תלויה בתצורת הרשת. כשהמחשב הוא חלק מקבוצת עבודה, עליך להשתמש בחלון User Manager הרגיל להוספת משתמשים לבסיס נתוני חשבונות המשתמש המקומי. כשהמחשב הוא חלק מתחום, יש להוסיף את המשתמש לבסיס נתוני חשבונות המשתמש של התחום באמצעות User Manager for Domains, המוצג בתרשים 15.2. בנוסף, בסיס הנתונים של התחום ניתן לעדכון רק מבקר התחום PDC או BDC, או ממחשב אחר שעליו מותקנת התוכנה לניהול תחומים.



תרשים 15.2: *תיבת הדו-שיח User Manager for Domains ב-Windows NT מאפשרת למנהל ליצור חשבונות משתמשים*

שם משתמש ב-Windows NT יכול להכיל עד 20 תווים הכוללים כל שילוב של מספרים, או תווים, מלבד התווים הבאים: " \ / : ; | = + * < >.

Windows NT מאפשרת למנהל הרשת לשלוט על הגדרות נוספות בחשבון המשתמש, כפי שמוצג בתרשים 15.3. מעבר למספר אפשרויות לבקרת סיסמה, המנהל יכול להגדיר אפשרויות לבקרת זמני כניסה לרשת (Hours), זכויות חיוג (לגישה לרשת מרחוק - dial-in) ולאילו קבוצות שייך חשבון המשתמש (יידון בהמשך בסעיף "חשבונות קבוצה").



תרשים 15.3: *מנהלי רשת Windows NT יכולים להגדיר פרטים בחשבונות משתמשים באמצעות תיבת הדו-שיח מאפייני המשתמש (User Properties)*

עדכון חשבונות משתמש

לאחר יצירת חשבון, צריך לעיתים לחזור ולעדכן מספר הגדרות. לדוגמה, שם משתמשת עשוי להשתנות לאחר שהיא נישאת, או שמשתמש יכול לעבור למחלקה אחרת ולהזדקק לעדכון שדה התיאור. רוב מערכות ההפעלה לרשת מאפשרות למנהל לעדכן חשבונות משתמשים באמצעות ממשק המשמש להוספת חשבונות משתמשים.

ב-Windows NT יכולים מנהלי רשת להשתמש ב- User Manager (או User Manager for Domains) לעדכון מידע אודות חשבונות משתמשים.

מכיון ש-Windows 9x אינה כוללת בסיס נתוני משתמשים, למעשה הפריט היחיד שניתן לשנות בהם הוא הסיסמה של חשבון משתמש. לשם כך המשתמש צריך להיכנס עם הסיסמה הנוכחית, לעבור ל**לוח הבקרה** (control panel) ולהשתמש באפשרות Passwords.

מחיקת חשבונות משתמש

לעיתים מתעורר צורך למחוק חשבון משתמש. לדוגמה, עובדים קבועים יכולים לעזוב את הארגון ועובדים זמניים יכולים לסיים את תקופת עבודתם. כדי למחוק חשבון משתמש, צריך מנהל הרשת לחזור ברוב המקרים את הממשק ששימש להגדרת המשתמשים. ב-Windows NT המנהל נכנס ל- User Manager המתאים (תרשים 15.2), בוחר את חשבון המשתמש ולוחץ על מקש Delete במקלדת. לאחר תיבת דו-שיח המאשרת את הפעולה, חשבון משתמש זה יימחק לחלוטין מבסיס נתוני חשבונות המשתמשים.



הערה: ב-Windows NT **ממופים חשבונות המשתמשים למספר זיהוי אבטחה** - SID (security identification number) **ייחודי, הנוצר עם הגדרת חשבון** המשתמש. **כל ההרשאות והבעלויות על קבצים מוקצות למעשה ל-**SID **ולא** לשם המשתמש. **אם תמחק בטעות חשבון משתמש ותנסה ליצור מחדש** משתמש באותו שם כמו הראשון, **לחשבון החדש יהיה** SID **אחר, וכברירת מחדל הוא לא יהיה חבר באותן קבוצות ולא יקבל את אותן הרשאות שקיבל המשתמש המקורי. לכן, לפני מחיקת חשבון משתמש ב-**Windows NT, **יש לשקול זאת היטב.**

מערכות הפעלה אחדות, כגון Windows NT וגרסאות UNIX רבות, מאפשרות למנהל ל**השבית** (disable) חשבון משתמש. החשבון אינו נמחק, אולם לא ניתן להשתמש בו לכניסה למערכת. עם Windows NT ניתן להשבית חשבון בעזרת User Manager או User Manager for Domains.

חשבונות קבוצה (Group Accounts)

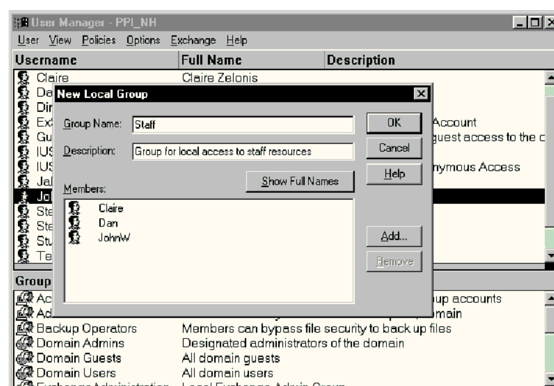
כאשר ברצונך לאפשר למספר משתמשים את הגישה למשאב רשת כלשהו, רוב מערכות הפעלת רשת מאפשרות להקצות הרשאת גישה לכל חשבון משתמש בנפרד. אולם, עם גידול מספר המשתמשים, שיטת בקרת הרשאות גישה זו הופכת למסורבלת. מערכות הפעלת רשת רבות כיום מאפשרות ליצור חשבונות **קבוצה**, להוסיף משתמשים לחשבון הקבוצה ולהקצות את הרשאות לחשבון הקבוצה (במקום לבצע זאת לכל אחד מהמשתמשים בנפרד).

לדוגמה, נניח שמחלקת משאבי אנוש רוצה להתיר גישה למספר תיקיות בשרת קבצים לחברי צוות משאבי אנוש בלבד. אם במחלקת משאבי אנוש היו עשרה משתמשים, יכולת להקצות הרשאת גישה לכל אחת מהתיקיות לכל חשבון משתמש. אולם, אם משתמש עוזב את מחלקת משאבי אנוש, תצטרך לפנות לכל אחת מהתיקיות ולהסיר מרשימת הגישה שלה את שם חשבון המשתמש. בשיטת חשבונות קבוצה תוכל ליצור חשבון קבוצה בשם HR (human resources), להגדיר את עשרת המשתמשים כחברים בקבוצה, ואז להקצות הרשאת גישה לכל תיקיה לחברי הקבוצה. כעת, כשמשתמש עוזב, צריך רק להסיר את שמו מרשימת חברי קבוצת HR, ואז הוא לא יוכל לגשת עוד לתיקיות המורשות לקבוצת HR.

רוב מערכות ההפעלה מאפשרות ליצור קבוצות בכפיפות למגבלות מתן שמות לקבוצות. בנוסף, חשבון משתמש יכול בדרך כלל להשתייך למספר חשבונות קבוצה.

במערכות הפעלה של מיקרוסופט, רק Windows NT מאפשרת ליצור קבוצות משתמשים. אם מחשבי Windows 95 הם חלק מתחום (Domain), הם יכולים להקצות הרשאות לקבוצות. אולם, לא ניתן ליצור קבוצות במחשב Windows 95 עצמאי.

יצירת חשבון קבוצה בתוך Windows NT נעשית כמו יצירת חשבון משתמש. בתרשים 15.4 תראה שרכיב User Manager (או User Manager for Domains) של Windows NT משמש ליצירת קבוצות. יוצרים חשבון קבוצה ואז מוסיפים לה את המשתמשים השייכים לה.



תרשים 15.4: *User Manager ב-Windows NT יכול לשמש גם ליצירת קבוצות באמצעות תיבת הדו-שיח New Local Group*

בעת פעולה בתוך תחום מאפשרת Windows NT ליצור **קבוצות מקומיות** (local) **וקבוצות גלובליות** (global). ל**קבוצות מקומיות** יש גישה רק למשאבים במחשב בו מוגדרת הקבוצה. לדוגמה, אם תיצור קבוצה מקומית הנקראת Staff עבור מחשב בשם ServerA, תוכל להקצות הרשאות גישה לקבוצה זו לכל תיקיה או מדפסת המחוברות ל-ServerA. אולם, כשתרצה להקצות הרשאות גישה לתיקיות הנמצאות על מחשב ServerB, הקבוצה Staff לא תהיה מוגדרת עבורו. תצטרך להגדיר קבוצה מקומית Staff חדשה עבור המחשב ServerB ולהקצות את האנשים המתאימים לקבוצה החדשה.

לעומת זאת, **קבוצות גלובליות** נראות בכל המחשבים שבתחום (Domain). כשתיצור קבוצה כללית Staff בבקר תחום ותוסיף את המשתמשים המתאימים, קבוצה זו תהיה זמינה לכל המחשבים. תוכל להקצות לקבוצה הגלובלית Staff את הרשאות הגישה לתיקיות שנמצאות הן ב-ServerA והן ב-ServerB.

Windows NT גם כוללת מספר קבוצות מובנות, כמו Administrators, Power Users, Users ו- Account Operators, המוגדרות מראש עם רמות גישה מתאימות אל משאבי המערכת.

חשבונות קבוצה ניתן לעדכן בדרך כלל בדומה לעדכון חשבונות משתמשים. Windows NT מאפשרת החלפת שם או מחיקת חשבון קבוצה באמצעות User Manager (או User Manager for Domains).

אבטחת רשת

הגנה על משאבי רשת יכולה להיות אחד התפקידים החיוניים ביותר של מנהל הרשת. אבטחת רשת אינה כרוכה בהגנת הרשת מפני גורמים חיצוניים בלבד, אלא גם הגנה על נתונים רגישים בתוך המערכת מפני משתמשים אחרים. בנוסף, קיימים משאבי רשת הדרושים לפעילות הרשת, שיש להגן עליהם מפני נזק מכוון או בשוגג.

ניתן להגדיר כך את תפקידך כמנהל רשת בהגנה על משאבי הרשת:

- ✯ יצירת מדיניות אבטחה (Security Policy) לארגון שלך,
- ✯ הקצאת הרשאות גישה מתאימות למשאבי רשת,
- ✯ ביקורת (פיקוח - Auditing) על אכיפת מדיניות האבטחה והרשאות הגישה.

מדיניות אבטחה (Security Policy)

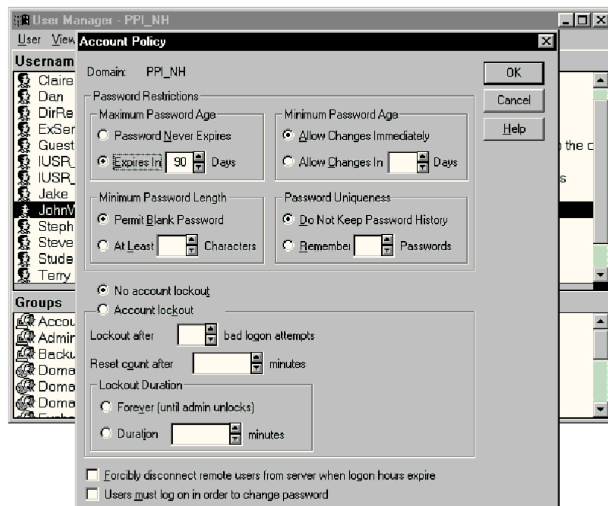
החלק הראשון בהגנת הרשת כרוך בהגדרת המותר והאסור למשתמשים. מדיניות אבטחה (security policy) מתוכננת היטב תתייחס לנושאים כגון:

- ✯ האם מותר למשתמשים להחליף סיסמאות? אם לא, כיצד יוקצו סיסמאות?
- ✯ באיזה סוג סיסמאות יכולים להשתמש? האם אפשר להשתמש במילה נפוצה, או שהסיסמה חייבת לכלול מספר או סימן?
- ✯ האם יפוג תוקפן של סיסמאות, דבר שיכריח משתמשים לשנות את הסיסמה שלהם? אם כן, כל כמה זמן?
- ✯ בעת החלפת סיסמאות, האם תרשה להשתמש בסיסמה שכבר השתמשו בה בעבר? או שצריך לספק סיסמה שונה בכל פעם שמחליפים סיסמה?
- ✯ מה אורכה של הסיסמה? האם תאשר סיסמה ריקה (blank)?
- ✯ באילו שעות יוכלו משתמשים להיכנס למערכת? האם יוכלו להיכנס לאחר שעות העבודה המקובלות?
- ✯ האם חשבון Guest (אורח) יהיה פעיל במערכת?

- אם יש קווי מודם לחיוג לרשת, למי מותר להתקשר ומתי אפשר לעשות זאת? האם משתמשים יוכלו להתקשר למערכת מכל קו טלפון, או האם המערכת תתקשר אליהם בחזרה (נוהל call back) למספר טלפון מסוים?
- האם ייעשה שימוש בהצפנת נתונים להגנה על מידע כלשהו?
- איזה חשבונות משתמשים ייכללו בכל חשבון קבוצה? מי יוכל לבצע פעולות ניהול, ובאיזו רמה הם יוכלו לפעול?
- למי יותר להיכנס למחשבים מיוחדים, כגון שרתים? מי יוכל לבצע פעולות ניהול כגון גיבוי נתונים, או הגדרת מדפסות?
- האם יותר למשתמשים להעתיק קבצים מדיסקטים אל השרת, או שיהיה צורך לבדוק תחילה כל קובץ נגד וירוסים?

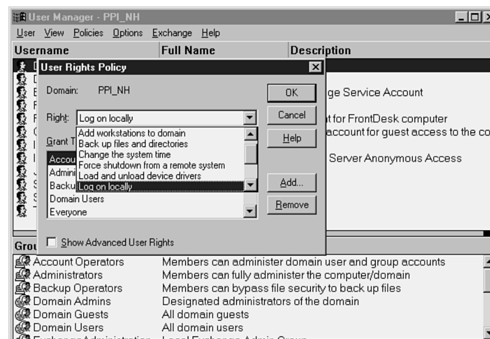
מדיניות האבטחה שלך תהיה תלויה במידה רבה ברגישות הנתונים, גודל הרשת, מספר החיבורים החיצוניים (כגון חיוג, או חיבור לאינטרנט) והמשאבים הזמינים, בנוסף לחששותיך הפרטיים בנושאי אבטחה. מדיניות אבטחה טובה תמצא איזון בין הצורך ברשת בטוחה לבין רצונך לשמור על יעילות העבודה. רשתות בטוחות במיוחד עשויות להוסיף שלבים למשימות שמשתמשים צריכים לבצע, ואילו רשתות המאפשרות למשתמשים לעשות ככל העולה על רוחם עשויות להישאר ללא אבטחה כלל.

מערכות הפעלת רשת אחדות מספקות כלים המסייעים למנהלים להגדיר ולאכוף מדיניות אבטחה. לדוגמה, Windows NT מאפשרת למנהלים להגדיר מדיניות בנושא אורך ותוקף סיסמה. מנהלים גם יכולים למנוע גישה ממשתמשים לאחר מספר כשלונות בניסיון כניסה למערכת. ב-Windows NT, פתח את User Manager (ראה תרשים 15.5) ובחר Account בתפריט Policies.



תרשים 15.5: *תיבת הדו-שיח Account Policy של Windows NT מאפשרת למנהל להגדיר מדיניות אבטחה בנושא סיסמאות*

בתרשים 15.6 תוכל לראות ש-Windows NT מאפשרת למנהל להקצות הרשאות לביצוע פעולות מערכת לחשבונות משתמש או קבוצה. לדוגמה, בקרי תחומים (Domain Controllers) מאפשרים למשתמשים לגשת למשאבים המשותפים שלהם על פני הרשת. אולם כברירת מחדל, גישה מקומית (ישיבה פיסית ליד בקר התחום וכניסה מקומית למחשב זה) מוגבלת לקבוצת Administrators (כדי להקצות הרשאות משתמש ב-Windows NT, פתח את User Manager ובחר User Rights מתפריט Policies).



תרשים 15.6: *תפריט User Manager ב-Windows NT מאפשר למנהלים להקצות הרשאות מערכת למשתמשים באמצעות תיבת הדו-שיח User Rights Policy*

הרשאות גישה (Access Permissions)

לאחר יצירת משתמשים וקבוצות והגדרת מדיניות אבטחה, צריך להקצות את ההרשאות המתאימות למשאבי הרשת. קיימים שני מודלים עיקריים להקצאת הרשאות גישה (access permissions):

- אבטחה ברמת השיתוף (share-level security),
- אבטחה ברמת המשתמש (user-level security).

אבטחה ברמת השיתוף (share-level)

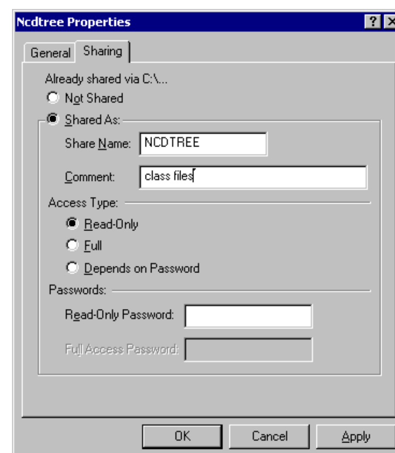
אבטחה ברמת השיתוף (share-level security) נקראת גם **שיתוף מאובטח-סיסמה** (password-protected shares), ולפיה מקצים סיסמה נפרדת **לכל משאב** רשת. אם המשתמש יודע את הסיסמה, הוא יכול להשתמש במשאב. אבטחה ברמת השיתוף נמצאת בדרך כלל ברשתות **שוויוניות** קטנות (עד עשרה משתמשים), כמו אלו שמשתמשות ב-Windows 9x. רשתות רבות מפעילות אבטחה ברמת השיתוף מכיון שהיא פשוטה וזולה. בסביבת מערכות הפעלה של מיקרוסופט כגון Windows 95, אין צורך בדבר נוסף מלבד מערכת ההפעלה הבסיסית. מכיון שכל משתמש יכול לשלוט באופן מלא על המשאבים שלו, לא דרוש צוות מרכזי לניהול הרשת.

עם הוספת משתמשים לרשת, הם יצטרכו לזכור מספר סיסמאות שונות ורבות כדי לגשת למשאבים המשותפים. בנוסף, כשרוצים להפסיק את הגישה של משתמש כלשהו למשאב מסוים, יש צורך להגדיר סיסמה חדשה ולהפיץ אותה לכל המשתמשים שעדיין מותרת להם הגישה למשאב זה.

מערכות הפעלת רשת אחדות מספקות דרגות שונות של אבטחה ברמת השיתוף. למשל, Windows 95 מאפשרת למשתמשים להקצות לתיקיה את סוגי האבטחה האלו :

- Read-Only (קריאה בלבד). משתמשים שיודעים את הסיסמה יכולים לראות ולהעתיק קבצים מהספריה, אך אינם יכולים לשנות את המסמכים שנמצאים בה.
- Full (מלאה). משתמשים שיודעים את הסיסמה מקבלים שליטה מלאה על כל הקבצים בתיקיה ויכולים להוסיף, למחוק, או לשנות כל קובץ.
- Depends on Password (תלוי בסיסמה). מוגדרות שתי סיסמאות לתיקיה המשותפת. אם משתמשים יודעים את הסיסמה המלאה, יש להם שליטה מלאה ; אם הם יודעים את הסיסמה לקריאה בלבד, תהיה להם גישה לקריאה בלבד.

תיבת הדו-שיח שבה ניתן להקצות דרגות אבטחה שונות ברמת השיתוף מוצגת בתרשים 15.7. שים לב ש-Windows 95 מאפשרת להשאיר את שדה הסיסמה ריק, מצב שמאפשר לכל המשתמשים לגשת לתיקיה המשותפת עם רמת האבטחה המוגדרת. לדוגמה, אם סוג ההרשאה Full אולם הסיסמה ריקה, כל משתמשי הרשת יקבלו גישה מלאה לתיקיה המשותפת.



תרשים 15.7: *תיבת הדו-שיח Class Properties ב-Windows 95 מתייחסת למאפייני תיקיה בשם class, מאפשרת למשתמשים להקצות סוגי אבטחה שונים ברמת השיתוף (share-level)*



רעיון מפתח

ברשת שבה נהוגה **אבטחה ברמת השיתוף** אין בחינת אימות ובקרה מרכזיים על משתמשים. ניתן להקצות למשאב סיסמה בעת שיתופו ברשת. למרות שלמשתמשים יש שליטה מקומית מלאה, הם צריכים לדעת את הסיסמה של כל אחד מהמשאבים המשותפים שאליהם הם רוצים לגשת במחשב המרוחק. מערכות Windows 9x יכולות להשתמש באבטחה ברמת השיתוף כאשר אינן חלק מתחום Windows NT Server

אבטחה ברמת המשתמש (user-level)

אבטחה ברמת המשתמש (user-level security) מוקצית על בסיס חשבון המשתמש, ולא כמו אבטחה ברמת השיתוף. משתמשים נכנסים למערכת באמצעות שם משתמש וסיסמה. כאשר הם מנסים להתקשר למשאב רשת, שם המשתמש והסיסמה נבדקים בבסיס נתונים מרכזי. אם יש אישור, המשתמשים מקבלים גישה מהסוג שהוקצתה להם.

בדרך כלל אבטחה ברמת המשתמש עדיפה ברשתות גדולות, מכיון שמשתמשים אינם צריכים לזכור סיסמאות נוסף לסיסמת הכניסה שלהם. משתמשים נכנסים לרשת ומתחילים להשתמש מייד במשאבים שאליהם הוקצתה להם גישה. אבטחה ברמת המשתמש גם נחשבת בטוחה יותר, מכיון שמשתמשים אינם נוטים להפיץ את סיסמת הכניסה העיקרית שלהם, וכאשר יש להם סיסמת גישה אחת בלבד, פוחתת הנטייה להציג את הסיסמה במקום בולט לעין לשם תזכורת.

ניהול משאבים משותפים רבים פשוט הרבה יותר בשיטת האבטחה ברמת המשתמש (user-level) מאשר באבטחה ברמת השיתוף (share-level). למשאבי רשת מוקצות הרשאות לפי משתמש, או לפי קבוצה. כאשר רוצים למנוע ממשתמש המשך גישה למשאב משותף, חשבון המשתמש שלו מוסר מרשימת ההרשאות של המשאב.

הבדל עיקרי בהשוואה לאבטחה ברמת השיתוף הוא שהרשאות למשאבי הרשת מוקצות על ידי מנהלים, או על ידי משתמשים אחרים בעלי הרשאות ניהול. לרוב משתמשי הרשת אין יכולת להגדיר הרשאות, או אפילו לשתף קבצים ומדפסות עם משתמשי רשת אחרים.

לסיום, בדרך כלל מערכות המשתמשות באבטחה ברמת המשתמש מספקות סוגי בקרת גישה רבים יותר מאשר בשיטת אבטחה ברמת השיתוף. לדוגמה, בעוד ש-Windows 95 מספקת שלושה סוגי בקרת גישה (אין גישה, קריאה בלבד, גישה מלאה), Windows NT מספקת שבעה סוגי בקרת גישה, כפי שמוצג בטבלה 15.1. ניתן לשלב הרשאות אלו כדי להקצות למשתמש הרשאות גישה מפורטות מאוד.

טבלה 15.1: הרשאות גישה לתיקיה/קובץ ב- Windows NT (הרשאות אינדיווידואליות)

Read (R) (קריאה)	המשתמש יכול לראות ולהעתיק קבצים בתיקיה.
Write (W) (כתיבה)	המשתמש יכול לעדכן קבצים בתיקיה.
Execute (X) (הרצה)	המשתמש יכול להריץ תוכניות בתיקיה.
Delete (D) (מחיקה)	המשתמש יכול למחוק קבצים בתיקיה.
Change Permission (P) (שינוי הרשאה)	המשתמש יכול לשנות את ההרשאות לקבצים.
Take Ownership (O) (לקיחת בעלות)	המשתמש יכול לקחת בעלות על קבצים.
No Access (אין גישה)	למשתמש אין גישה לקבצים, ואף אינו יכול לראות את תוכן התיקיה.

בעת שיתוף קבצים, Windows NT משלבת הרשאות גישה אלו ליצירת ארבע רמות של אבטחה ברמת המשתמש (הרשאות סטנדרטיות):

- No Access (אין גישה). למשתמשים אין גישה כלל למשאב המשותף.
- Read (RX) (קריאה). משתמשים יכולים לראות או להעתיק קבצים ולהריץ יישומים.
- Change (RWXD) (שינוי). משתמשים יכולים לראות, לעדכן, להוסיף או למחוק קבצים בנוסף להרצת יישומים.
- Full Control (RWXDOP) (שליטה מלאה). למשתמשים יש הרשאות מנהלים לגישה לקבצים בתיקיה.

ניתן להקצות כל סוג של בקרת גישה למשתמש מסוים או לחשבון קבוצה, בהתאם להגדרות הרשאות משתמשים.



הערה: **חלק מהגדרות הרשאות אלו תלויות בסוג מערכת ניהול הקבצים (disk file system) שבשימוש ובנוהלי מדיניות מערכת אחרים של Windows NT. למרות שדיון מלא בהגדרת הרשאות Windows NT הוא מעבר לגבולות ספר זה, טבלה 15.1 ניתנת כאן כדוגמה.**

לאבטחה ברמת המשתמש (user-level) יש מספר חסרונות. לדוגמה, מכיון שאבטחה ברמת המשתמש מסתמכת (בסביבת תחומים) על בקרי תחומים (Domain Controllers) לאימות משתמשים, כל כשל בבקרי התחומים עלול להשאיר את כל המשתמשים ללא אפשרות כניסה למערכת או ללא אפשרות גישה למשאבי המערכת. בנוסף, משתמשים העוברים למערכות המשתמשות באבטחה ברמת המשתמש ממערכות עם אבטחה ברמת השיתוף, עלולים להתלונן על חוסר השליטה שלהם בשיתוף משאבים והגדרת הרשאות.

עם זאת, אבטחה ברמת המשתמש בעלת האבטחה המשופרת, הגישה וניהול משאבים קל יותר, היא המודל השולט במערכות רשת מבוססות שרת (server based). במערכות הפעלה של מיקרוסופט, אבטחה ברמת המשתמש היא המודל העיקרי ב-Windows NT (עבור מחשבים מרושתים ועבור מחשבים בודדים) וניתן להשתמש בה גם במערכות Windows 9x כאשר הם חלק מתחום. מחשבי Windows 95 יכולים גם לממש אבטחה ברמת המשתמש על ידי שימוש בבסיס נתוני חשבונות המשתמשים על מחשב Windows NT בודד שאינו חלק מתחום.



רעיון מפתח

רשת המשתמשת באבטחה ב**רמת המשתמש** (user-level) כוללת שרת מרכזי המכיל רשימת כל חשבונות המשתמשים לצורך בחינת אימות מרכזית (authentication) של המשתמשים. ברשתות אלו צריכים המשתמשים לדעת סיסמה אחת בלבד כהרשאת כניסה לרשת. לאחר מכן, הם מורשים להשתמש בכל משאבי הרשת שעבורם הוקצתה להם הרשאת גישה. רשתות Windows NT Server משתמשות באבטחה ברמת המשתמש.

ביקורת (Auditing)

מרכיב נוסף להגנה נאותה על הרשת הוא מעקב אחר אירועי אבטחה במחשב שלך. **ביקורת** (auditing) מתייחסת לתהליך המעקב אחר פעילויות בחשבונות משתמשים ואירועי רשת אחרים. **יומן ביקורת** (audit log) יכול לספק מידע אודות פעילות המשתמשים במערכת, מי מנסה להתחבר למערכת ואילו משאבי מערכת נמצאים בשימוש רב. יומני ביקורת יכולים לעזור למנהל לגלות פעילות לא מורשית, או לקבוע אם גורמים זרים מנסים לחדור למערכת.

בדרך כלל יומני ביקורת עוקבים אחר אירועים כגון אלה:

- ✯ הצלחה וכישלון של ניסיונות כניסה ויציאה מהמערכת,
- ✯ התקשרות למשאבי רשת,
- ✯ סגירה או הפעלה מחדש של המערכת,
- ✯ שינויים לקבצים או תיקיות,
- ✯ שינוי סיסמה,
- ✯ הוספה או מחיקה של חשבונות משתמש או קבוצה,
- ✯ שינוי הרשאות לקבצים או תיקיות,
- ✯ פתיחה או סגירה של קבצים,

בתרשים 15.8 תוכל לראות מערכות הפעלה אחדות שמספקות כלים גרפיים להצגת נתונים מיומני ביקורת. את נתוני יומן הביקורת תוכל להעביר גם ליישומים אחרים שבעזרתם ניתן לסנן או להציג תרשימים בצורות ובחתכים שונים.

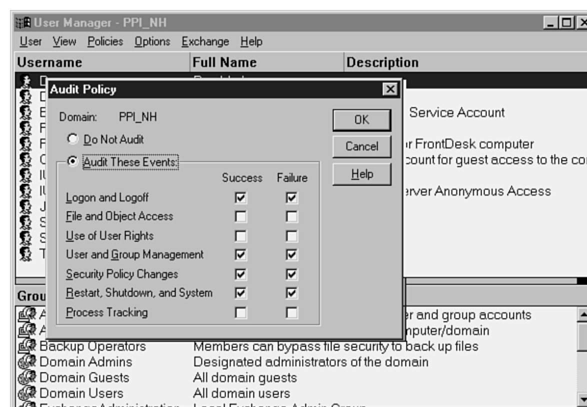
Event Viewer - Security Log on \\HAWK

Log View Options Help

Date	Time	Source	Category	Event	User
4/4/97	10:54:42 AM	Security	Logon/Logoff	528	Dan
4/4/97	9:22:31 AM	Security	Logon/Logoff	538	Dan
4/4/97	9:14:22 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:14:12 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:11:05 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:11:05 AM	Security	System Event	515	SYSTEM
4/4/97	9:08:06 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:07:17 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:02:53 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:00:53 AM	Security	Logon/Logoff	528	Dan
4/4/97	9:00:42 AM	Security	Logon/Logoff	529	SYSTEM
4/4/97	9:00:42 AM	Security	System Event	515	SYSTEM
4/4/97	8:39:44 AM	Security	Logon/Logoff	538	Dan
4/4/97	8:29:36 AM	Security	Logon/Logoff	528	Dan
4/4/97	8:05:16 AM	Security	Logon/Logoff	538	Dan
4/4/97	7:52:15 AM	Security	Logon/Logoff	528	Dan
4/4/97	7:52:15 AM	Security	Logon/Logoff	528	Dan
4/3/97	3:09:24 PM	Security	Logon/Logoff	538	Jake
4/3/97	3:09:21 PM	Security	Logon/Logoff	528	Jake
4/3/97	6:22:07 AM	Security	Logon/Logoff	538	Dan
4/3/97	6:22:05 AM	Security	Logon/Logoff	538	Dan

תרשים 15.8: *Event Viewer של Windows NT מאפשר למנהל לראות יומני ביקורת של מערך האבטחה*

במערכת Windows NT ניתן להפעיל את מנגנון הביקורת על ידי בחירת Audit מתפריט Policies שב- User Manager (או User Manager for Domains). בתרשים 15.9 תוכל לראות שניתן להגדיר את אירועי המערכת שיבוקרו.



תרשים 15.9: *בתיבת הדו-שיח Audit Policy של User Manager ניתן להגדיר איזה אירועי מערכת ישתתפו בביקורת*

סיכום

לאחר התקנת הרשת, תפקידך כמנהל רשת רק מתחיל. ככל שהרשת ממשיכה לפעול, מנהל הרשת צריך ליצור משאבי רשת חדשים, לנהל משאבי רשת קיימים, ולאבטח את הרשת מפני גישה לא מורשית.

חלק ניכר מפעילות ניהול הרשת קשור ביצירת חשבונות משתמשים והקצאת הרשאות למשאבי רשת. במערכות הפעלה של מיקרוסופט ניתן לבצע משימות אלו לפי קבוצת עבודה או תחום. קבוצת עבודה היא קבוצה לוגית של מחשבים ברשת שוויונית. תחום משתמש במודל מבוסס-שרת, שבו ניהול חשבונות המשתמשים נעשה מאתר מרכזי.

מנהלי רשתות יכולים ליצור חשבונות משתמשים באמצעות ממשק גרפי ולכלול ברשימה שלהם מידע נוסף אודות המשתמשים. לרוב מערכות ההפעלה לרשת יש חשבונות משתמשים מיוחדים המאפשרים גישה ניהולית למערכת, וחשבונות אחרים המאפשרים גישה לאורחים.

במערכות המשתמשות באבטחה ברמת המשתמש ניתן ליצור חשבונות קבוצה שניתן להקצות להם הרשאות. חשבונות קבוצה מספקים מנגנון להקבצה לוגית של משתמשים בעת הקצאת הרשאות.

אחריות עיקרית נוספת של מנהל הרשת היא אבטחת הרשת. אבטחת הרשת כרוכה בהגדרת מדיניות אבטחה, הקצאת הרשאות הגישה המתאימות למשאבי הרשת, ובקרה על אירועי הרשת.

מדיניות אבטחה טובה מאזנת בין הצורך באבטחת הרשת לבין הצורך של המשתמש בתפוקה סבירה. מדיניות אבטחה תכלול נושאים כגון התיישנות סיסמאות, הגבלת זמני כניסה, חשבונות אורח וזכויות ניהול. מערכות הפעלה אחדות, כמו למשל Windows NT מספקות כלים גרפיים להגדרת מדיניות אבטחה.

בעת הקצאת הרשאות גישה למשאבי רשת קיימים שני מודלים לאבטחה. בשיטת אבטחה ברמת השיתוף מוקצית סיסמה לכל משאב רשת משותף. אם המשתמש יודע את הסיסמה, הוא יכול לגשת למשאב. כל משתמש במחשב אחראי לתחזוקה ולאבטחה של המחשב שלו. בשיטת אבטחה ברמת המשתמש, הגישה מורשית על בסיס המשתמש כמובן. כאשר משתמש מנסה להתחבר למשאב רשת, שם המשתמש והסיסמה שלו נבחנים ומאומתים בבסיס נתונים מרכזי.

לסיום, חלק מאבטחת הרשת כרוך בשימוש בתוכניות ביקורת למעקב התקשרויות למחשב והשימוש במשאבים משותפים. יומני ביקורת יכולים לספק אמצעי לזיהוי גישה בלתי מורשית לרשת.

16

מניעת תקלות ברשת

נוסף לניהול חשבונות משתמשים ושמירה על אבטחת הרשת, מנהלי רשתות אחראים גם למנוע אובדן נתונים ולמנוע תקלות ברשת לפני התרחשותן. עד סוף הפרק תוכל:

- ✯ להבין את התפקיד של תיעוד נאות במניעת תקלות ברשת,
- ✯ להסביר איזה כלים זמינים לבקרת ביצועי הרשת וכיצד הם יכולים לסייע במניעת תקלות,
- ✯ לתאר כיצד אל-פסק (UPS) יכול להקל בעת תקלות אספקת מתח,
- ✯ להבין כיצד מערכת גיבוי יכולה למנוע אובדן נתונים,
- ✯ לזהות סוגים שונים של אמצעי דיסק אחסון עמידים בפני תקלות,
- ✯ להסביר את השימוש בתוכניות התאוששות מאסון.

הגנת הרשת

כמנהל רשת, אחת המשימות העיקריות היא להגן על הרשת מפני אובדן נתונים ולמנוע תקלות ברשת לפני התרחשותן. הצעדים הכרוכים במניעת תקלות ברשת כוללים:

- ✯ תיעוד נאות של תצורת הרשת,
- ✯ ניטור (monitoring) ביצועי הרשת,
- ✯ גיבוי נתונים,

* אספקת מנגנוני חומרה למניעת כשל ציוד,
* פיתוח תוכנית מקיפה להתאוששות מאסון.

כל אחד מצעדים אלה יידון בפירוט בסעיפים הבאים.

תיעוד (Documentation)

הצעד הראשון במניעת תקלות רשת הוא תיעוד ההתקנה והגדרת התצורה של הרשת. תיעוד הרשת צריך לכלול מידע אודות חיבורי LAN ו-WAN. אם אתה אחראי על רשת גדולה יותר המקיפה מספר רשתות מקומיות נפרדות, צריך להיות לכל רשת מקומית תיעוד נפרד. בנוסף, עליך לעדכן כל העת את התיעוד, כדי שיכלול את השינויים האחרונים שנעשו בתצורת הרשת.

למרות שמרכיבי מערכת תיעוד משתנים, הרשימה הבאה כוללת מידע שכדאי לתעד:

* **מידע התקנת כבלים**. איזה סוג של כבל רשת מותקן ברשת המקומית? האם יש שרטוטי רשת המתארים את החיבורים בין תקעים בקיר לבין תקעים בלוח החיבורים (patch panel) שבארון חיווט? האם יש מספרי טלפון כדי להתקשר לאנשים האחראים על ההתקנה עצמה? לאיזו מהירות עבודה מדורג הכבל?
* **מידע ציוד**. מתי נרכשו פריטי הציוד השונים (מחשבים אישיים רגילים וציוד מיוחד לרשת)? מהם המספרים הסידוריים? מי היו הספקים? האם יש מידע כיצד להתקשר אל הספקים? האם יש מידע בנושא אחריות?
* **תצורת תוכנה**. איזו תוכנה מותקנת בכל צומת רשת? איזה דרייברים היה צריך לטעון, כדי שהמחשב ייגש בהצלחה לרשת? איזה קבצי תצורה (כגון CONFIG.SYS ו-AUTOEXEC.BAT) טעונים בכל מחשב, ואילו הוראות מיוחדות נכללות בהם? האם מופעלים ברשת יישומים יוצאי דופן, או שיש בה הגדרות מיוחדות?
* **משאבי רשת**. מהם משאבי הרשת שהשימוש בהם שכיח ביותר ברשת? האם יש מיפויי כונן מסוימים שבהם ברצונך להשתמש ברחבי הרשת?
* **כתובות רשת**. כיצד הקצית כתובות רשת? האם אתה יכול לספק מפה או תרשים של המחשבים ואילו כתובות הוקצו להם?
* **חיבורי רשת**. האם הרשת מחוברת לרשתות אחרות? אם כן, כיצד? מי הם ספקי השירותים? האם יש מידע כיצד להתקשר עם ספקי השירותים?
* **ביצועי הרשת**. מהן רמות התעבורה ה"רגילות" ברשת? היכן צווארי הבקבוק האופייניים לביצועי הרשת?
* **ניהול משתמשים**. האם יש שיטה קבועה ליצירת שמות משתמשים? האם יש קבוצות מסוימות שאליהן צריך לצרף את כל המשתמשים?
* **מדיניות ונהלים**. האם אתה, או חבר בארגון, הגדרתם והפצתם נהלים מסוימים לפעילות הרשת? האם ההנהלה הבכירה התוותה קווים מנחים לשימוש ברשת?

- **שינויי חומרה/תוכנה**. איזה שינויים בוצעו מאז התקנת הרשת? מתי התרחשו שינויים אלה?
- **רשיונות שימוש בתוכנה**. האם יש רשיונות תקפים לכל התוכנה המותקנת באתר שלך? האם כל המספרים הסידוריים רשומים ונמצאים תחת מעקב תאריך תפוגה?
- **מעקב איתור ותיקון תקלות**. אילו בעיות היו בעבר ברשת, וכיצד פתרת אותן?

ערכת תיעוד המתארת פריטים כגון אלה המופיעים ברשימה זו עשויה להיות מועילה מאוד כאשר מנסים לאבחן בעיות ברשת. בעת תכנון הגדלת הרשת או עדכון פריטי ציוד, תמצא שהתיעוד יכול לסייע בקידום השינויים המתוכננים.

שים לב שהתיעוד צריך להיות זמין בנייר מודפס, ולא רק בקובץ מחשב, עבור אותם מקרים שהרשת אינה נגישה.



הערה: המורכבות הגדלה והולכת של רשתות חייבה ספקים רבים לפרסם כלי ניהול עבור המערכת הכוללת, שגם מסייעים להכין תיעוד של תצורת הרשת. תרומת מיקרוסופט לתחום זה היא תוכנת שרת ניהול מערכת - מערכת Systems Management Server (SMS) הנכלל כחלק מ- Microsoft BackOffice. תוכנה זו יכולה לבנות בסיס נתוני מלאי, על ידי איסוף מידע אודות הנתונים המאוחסנים בכל מחשב בארגון. לאחר איסוף המידע, שרת SMS יכול להתקין ולהגדיר תוכנה חדשה ישירות במחשבי הלקוח השונים ברשת. הוא גם יכול לספק פונקציות בקרת רשת מתקדמות לניתוח תעבורת הרשת.

ניטור ביצועי הרשת (Network Performance Monitoring)

תיעוד המערכת מאפשר לך גם להמשיך וללמוד כיצד המערכת מתפקדת באופן סדיר. כדי לרכוש יכולת זו, תצטרך להשתמש במספר כלי בקרת ביצועים. למנהלי רשתות יש מספר סיבות לניטור ביצועי הרשת, ביניהן:

- זיהוי התקנים המהווים צוואר בקבוק (bottleneck),
- אספקת נתונים לחיזוי צורכי גידול בעתיד ותכנון קיבולת,
- פיתוח תוכניות לשיפור ביצועי הרשת,
- בקרת השפעות שינויים בהגדרות חומרה או תוכנה,
- זיהוי מגמות בתעבורת רשת.

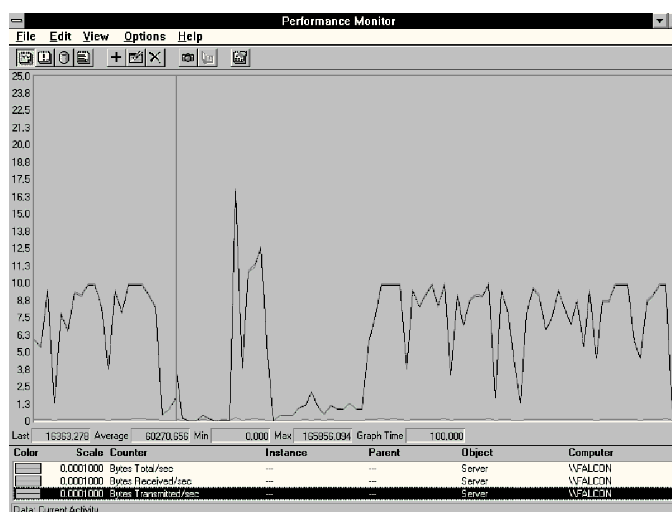
לפי רשימה זו תוכל להסיק שמנהלי רשתות מבלים את רוב זמנם באיתור צווארי בקבוק. **צווארי בקבוק** (bottlenecks) הם מצבים שמסיבה כלשהי גורמים להשהיות בזרימת התעבורה ברשת ולפגיעה בעבודת המשתמשים. צווארי בקבוק מתפתחים במקרים רבים ברכיבים שבתוך מחשבי שרת, כמו מעבדים, זיכרון (RAM), כרטיסי ממשק רשת (NIC) ובקרי דיסק. עם זאת, צווארי בקבוק יכולים גם להיות בתווך הרשת, או בהתקני קישוריות, כמו נתבים ושערים. בדרך כלל צוואר בקבוק נוצר כשלהתקן אין קיבולת מספקת כדי להתמודד עם נפח תעבורת הרשת שבו הוא נתקל.

למרות שבקרת ביצועים יכולה לסייע בראיית תנאי הרשת בהווה, היא לא תסייע בזיהוי בעיות אפשריות ברשת, אם לא תבסס תחילה **נקודת מוצא**, או **קו בסיס** (baseline) המגדירים פעולות רשת "רגילות". אם תְּנַטֵר את הרשת במשך פרק זמן שבו אין תקלות, תוכל להשתמש בפרק זמן זה כקו בסיס להשוואה, כאשר תנסה מאוחר יותר לזהות תקלות. כיצד תדע שתעבורת הרשת עמוסה אם לא תדע מה היו רמות התעבורה קודם לכן? כיצד תדע שהמעבד עובד קשה מדי אם אינך יודע את רמות הפעילות הרגילות שלו? קביעת קו בסיס יסייע בהתייחסות לנושאים אלה.

Windows NT Performance Monitor

רוב מערכות הפעלת הרשת כוללות כלי גרפי כלשהו לניטור ביצועי הרשת. כלים מסוג זה מספקים בדרך כלל מנגנון לתצוגת הנתונים כרשימת יומן וגם כתרשים גרפי.

בתוך Windows NT, הרכיב Performance Monitor (**מנטר הביצועים**) מאפשר ניטור גרפי של סטטיסטיקת הביצועים ברוב ההיבטים של פעילות המחשב, כפי שמוצג בתרשים 16.1. תוכל לראות את הנתונים בזמן אמיתי, או לאסוף אותם לקבצי יומן (Log Files) לניתוח מאוחר יותר. בנוסף לתרשימים גרפיים, Performance Manager יכול גם לספק רשימות של קבצי יומן ודוחות טקסט רגילים.



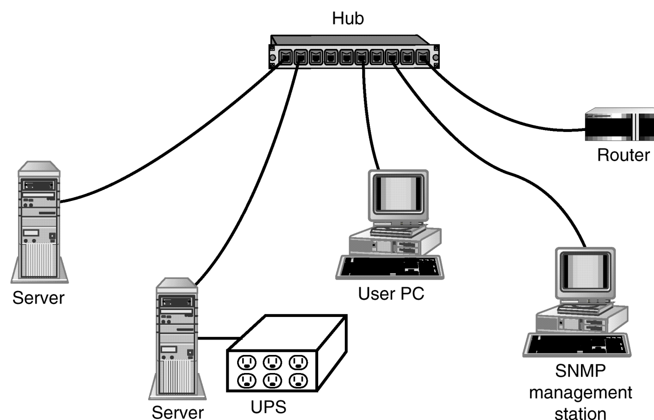
תרשים 16.1: *Performance Monitor של Windows NT מאפשר ניטור של סטטיסטיקת ביצועי הרשת מתוך מחשב השרת*

כאשר מתקיימים תנאים מסוימים, Performance Monitor יכול לשלוח התראה למנהל הרשת או להפעיל תוכנית אחרת.

SNMP

אחד הכלים העומדים לרשותך לניטור הרשת הוא Simple Network) SNMP Management Protocol). SNMP הוא תקן הנתמך על ידי רוב יצרני ציוד רשת, כולל יצרני רכזות (Hubs), כרטיסי ממשק רשת (NIC), נתבים (Routers), שרתים (Servers), גשרים (Bridges) וציוד רשת אחר.

כאשר נעשה שימוש ב-SNMP בסביבה כמו זו המוצגת בתרשים 16.2, נטענים **סוכני תוכנה** (software agents) בכל התקן רשת שינוהל. כל סוכן כזה (רכיב תוכנה) מנטר הן את תעבורת הרשת והן את מצב ההתקן ואוגר מידע זה ב**בסיס נתוני ניהול** (Management Information Base).



תרשים 16.2: *SNMP מאפשר ניהול התקני רשת מתחנת ניהול מרכזית*

כדי לאסוף ולהבין את כל המידע, תוכנת ניהול רשת מיוחדת דוגמת (polls) באופן סדיר את ההתקנים ואוספת את הנתונים שנאגרו בכל MIB. תוכנית הניהול יכולה לשלב את הנתונים מכל ההתקנים ולחולל סטטיסטיקה או תרשימים המפרטים את מצב הרשת הנוכחי. ניתן להגדיר ערכי סף שיפעילו התראות שיישלחו למנהלי הרשת כאשר יש עליה מעל רמות מסוימות שנקבעו. רכיבי רשת אחדים המפעילים SNMP גם ניתנים לניהול מרחוק, באמצעות תוכנת ניהול הרשת.



רעיון מפתח

SNMP (Simple Network Management Protocol) מספק מנגנון המאפשר למנהלי רשת לאסוף נתונים מרכיבי הרשת ולפתח תמונה כוללת של מצב הרשת.

מערכות גיבוי (Backup)

כאשר תשקול שיטות למניעת אובדן נתונים, המנגנון הקל ביותר להגנה בפני תקלה כזו הוא שימוש **במערכת גיבוי** (backup system) כלשהי. הצעדים הדרושים לפיתוח תוכנית גיבוי אמינה כוללים:

1. קביעת המידע החיוני שנמצא ברשת וזקוק לגיבוי.
2. פיתוח לוח זמנים לגיבוי נתונים. בדרך כלל, נתונים שאינם משתנים ניתן לגבות לפי לוח זמנים קבוע, ואילו נתונים קריטיים המשתנים כל הזמן יש לגבות בכל יום. מכיון שמערכות גיבוי משפיעות לרוב על ביצועי הרשת, יש לתזמן גיבויים לשעות שבהן השימוש ברשת מועט.
3. זיהוי האיש (או האנשים) שיהיה אחראי לתחזוקת גיבויים, והבטחה שהוא מבין את האחריות המוטלת עליו.
4. בחירת כונן סרט מגנטי לגיבוי. רוב מערכות הגיבוי משתמשות בכונני סרט עם מחסנית הניתנת להחלפה. סוג כונן הסרט שתבחר יהיה תלוי בנפח הנתונים לגיבוי, המהירות הדרושה לפעולת הכונן והעלויות הכרוכות הן בכונן והן בתווך. באופן אידיאלי תרצה להעתיק את כל נתוני הגיבוי אל סרט יחיד, או מספר קטן של סרטים. נושא נוסף שיש להתייחס אליו הוא יכולת העברת התווך, מחסנית הסרט, אל מערכות אחרות. במקרה של תקלה חמורה במחשב שלך, האם סוג כונן הסרט והמחסנית שבחרת יאפשרו לך להמשיך בעבודה במחשב אחר שישמש לך כמחשב גיבוי, אשר בו תוכל לשחזר במהירות את הנתונים?



הערה: כיום משתמשים לגיבוי גם בתקליטורים מסוג CD-R או PD. התקליטור יכול להכיל עד 650MB והוא התקן אמין ונוח.

5. קביעת השיטות לגיבוי הנתונים. כפי שמוצג בטבלה 16.1, קיימות מספר שיטות לגיבוי נתונים. מערכת גיבוי אמינה תשתמש בשילוב שיטות, וייתכן שתבצע גיבוי מלא פעם בשבוע, עם גיבוי דיפרנציאלי או אינקרמנטלי (תוספתי) בכל יום.
6. בדיקת מערכת הגיבוי. הרץ מספר סבבים של גיבוי הנתונים. הנח תמיד שחלק מהנתונים נמחקו (העבר אותם לספריה אחרת) ובדוק את יכולתך לשחזר במהירות את הנתונים. לאחר הפעלת מערכת הגיבוי, בדוק אותה באופן סדיר כדי להבטיח גיבוי אמין של הנתונים.
7. זיהוי אתרי אחסון באתר ומחוץ לאתר. באתר, גיבויי נתונים צריכים להיות מאוחסנים במקום נגיש בקלות. כדאי גם לאחסן סרטי גיבוי ותקליטורי גיבוי (מסוג CD-R או PD) במקום שמחוץ לאתר. המקום החלופי צריך להגן על הנתונים וממנו ניתן יהיה לשחזר את הנתונים בסרטים ובתקליטורים לאחר אסון. צריך להבטיח שרק לעובדים מורשים תהיה גישה לסרטי הגיבוי והתקליטורים, הן באתר והן מחוץ לו.

8. תחזוקת יומן גיבוי (Backup Log) מקיף המציין איזה נתונים מגובים, מתי בוצע הגיבוי, ומי ביצע אותו. יש לכלול גם מספרי זיהוי המציינים בבירור איזה סרט או תקליטור שימשו לגיבוי.

אם תפתח מערכת גיבוי הכוללת צעדים אלה, תהיה מוכן למניעת אובדן נתונים ברוב המצבים.

טבלה 16.1: *שיטות גיבוי*

שיטה	תיאור
Full Backup (גיבוי מלא)	גיבוי כל הקבצים שנבחרו, בין אם השתנו מאז הגיבוי האחרון ובין אם לא השתנו, וסימונם כקבצים שגובו.
Copy (העתקה)	גיבוי כל הקבצים שנבחרו, מבלי לסמן אותם כקבצים שגובו.
Incremental (תוספתי)	גיבוי וסימון קבצים נבחרים, רק אם שונו מאז הגיבוי האחרון.
Daily Copy (העתק יומי)	גיבוי כל הקבצים ששונו ביום נתון, בלי לסמן אותם כקבצים שגובו.
Differential (דיפרנציאלי)	גיבוי קבצים נבחרים רק אם השתנו מאז הגיבוי האחרון, אולם ללא סימון הקבצים כקבצים שגובו.

ביאור שיטות גיבוי

לשם הסבר ההבדלים שבין שיטות הגיבוי שתוארו בטבלה 16.1, נבחן לוח זמנים של מערך גיבוי אופייני ונציג גיבוי בסרט מגנטי, אך ההסבר מתאים גם לגיבוי בתקליטור: סרט 1 משמש לגיבוי מלא בכל יום ראשון בערב, וסרטים 2 עד 7 משמשים לגיבוי אינקרמנטלי (תוספתי) בשאר ימות השבוע. ביום שני, מגבים בסרט 2 את הקבצים ששונו מאז הגיבוי המלא שנעשה ביום ראשון בערב. ביום שלישי, מגבים בסרט 3 את כל הקבצים ששונו מאז הגיבוי האינקרמנטלי שנעשה ביום שני בערב, וכך הלאה. אם יש כשל בשרת הקבצים ביום שישי, צריך יהיה לשחזר תחילה את הנתונים מהגיבוי המלא שבסרט 1. אחר כך, צריך לשחזור נתונים מכל אחד מהסרטים 2 עד 5 (שנעשו בימים שני עד חמישי בערב), כדי לחזור למצב הקבצים לפני הכשל.

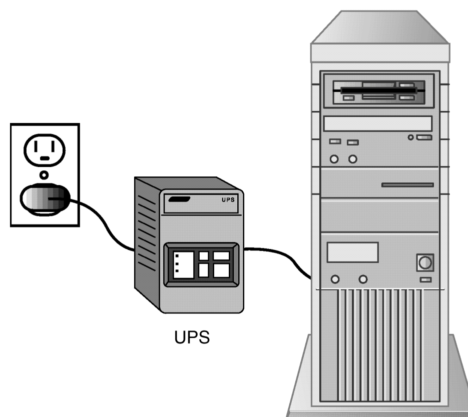
למרות שמערכת גיבוי זו מספקת רמה גבוהה של אבטחת נתונים, היא דורשת שמישהו יחליף את הסרט לפני כל גיבוי שנעשה. אם מישהו לא יחליף את הסרט, נתוני גיבוי יאבדו כי נתונים חדשים ייכתבו עליהם. לדוגמה, אם סרט 2 נשאר בכונן ביום שלישי, הנתונים ששונו ביום שלישי יירשמו עליו וידרסו את הנתונים שנשמרו בו ביום שני. לכן יש להחליף את הסרט בכל יום.

בסביבה משרדית קטנה יותר, הדבר אינו בהכרח מעשי. מערכת קטנה יותר תשתמש בסרט 1 לגיבוי מלא ביום ראשון בערב, ואחר כך תשתמש בסרט 2 לגיבויים דיפרנציאליים בשאר ימות השבוע. ביום שני בערב, סרט 2 יגבה את כל הקבצים ששונו מאז הגיבוי המלא ביום ראשון. ביום שלישי סרט 2 יגבה שוב את כל הקבצים ששונו מאז הגיבוי המלא ביום ראשון. אם תתרחש תקלה ביום שישי, יהיה צורך לשחזר תחילה את הנתונים מסרט 1 של הגיבוי המלא, ואחר כך רק מסרט 2. למרות שמערכת זו פשוטה יותר מהמערכת האינקרמנטלית שתוארה קודם, היא פחות אמינה. אם משהו קרה ביום חמישי וסרט הגיבוי לא תיפקד כראוי, כל הנתונים שהיו בו מאז הגיבוי המלא של יום ראשון יאבדו.

לסיום, עליך לשים לב להתקנת כונן סרט הגיבוי, או תקליטור הגיבוי, כדי להבטיח מהירות גיבוי בנוסף להשלכות מערכת הגיבוי על הרשת. המצב הטוב ביותר הוא להתקין את כונן הסרט על השרת עצמו. אם כונן הגיבוי יותקן במקום אחר ברשת, הוא ייצור תעבורת רשת רבה ועומס מיותר, כי למעשה מעתיקים את כל תכולת הכונן הקשיח שבשרת, או חלקים ממנו, אל כונן הגיבוי. אם יש צורך לגבות מספר שרתים באמצעות כונן סרט יחיד, מתקינים לעיתים מקטע רשת נפרד המשתמש בכרטיס ממשק רשת שני בכל שרת. עם מקטע רשת שני, כל תעבורת הרשת לגיבוי לא תשפיע על זרימת הנתונים העיקרית ברשת.

אל-פסק (Uninterruptible Power Supply)

מכיון שאפילו התנודה הקטנה ביותר במתח החשמלי עלולה לגרום אסון ברשת, מתקינים **אל-פסק**, Uninterruptible Power Supply) UPS), כדי לתמוך בעבודה רציפה ובלתי מופרעת מתנודות זרם. למעשה, התקן אל-פסק אינו אלא סדרת מצברים (במקרים אחדים, לא שונים בהרבה ממצברי מכונית) המספקים גיבוי לציוד הרשת במקרה של תקלה באספקת המתח. כפי שמוצג בתרשים 16.3, התקן אל-פסק מחובר לשקע החשמל בקיר (זרם חילופין) והשרת וציוד נוסף מחוברים אליו (ומקבלים זרם ישר). כאשר יש הפסקת מתח, מערכת אל-פסק ממשיכה לספק מתח לציוד המחשב. רוב מערכות האל-פסק מתוכננות לספק מתח לפרק זמן שבין 5 ל-20 דקות, אולם מערכות יקרות יותר יכולות לספק מתח למשך מספר שעות.

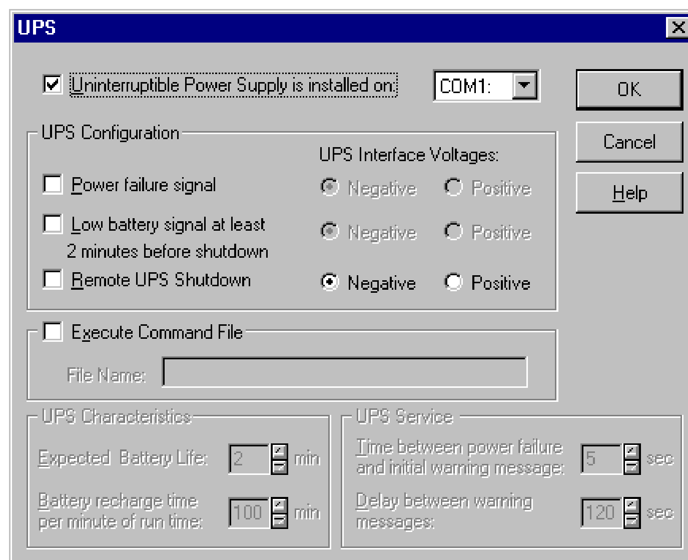


תרשים 16.3 *: מערכת אל-פסק (UPS) מחוברת בין שקע החשמל לבין מחשב השרת*

מערכות UPS מסווגות כמערכות **מקוונות** (online) או מערכות **כוננות** (standby). מערכות אל-פסק בכוננות (standby UPS) מעבירות את המתח מהשקע שבקיר ישירות לציוד המחשב המחובר אליהן, ובאותו זמן שומרות על טעינה מלאה של מצברי המערכת. כאשר יש הפסקה באספקת החשמל, מערכת זו מופעלת ומתחילה לספק מתח לציוד המחשב. אולם עלולה להיות נפילת מתח רגעית במהלך הפעלת מערכת האל-פסק, אשר עלולה לגרום במקרים מסוימים לאובדן נתונים. היתרון העיקרי של מערכת כוננות הוא במחירה הנמוך, בדרך כלל.

מערכות אל-פסק מקוונות (online UPS) משתמשות באספקת המתח מהשקע שבקיר לטעינה רציפה של המצברים שלהן, ומספקות את כל המתח לציוד המחשב ישירות ממצברים אלה. כאשר מתרחשת הפסקת חשמל, ציוד המחשב לא ירגיש בהפרעה, מכיון שהוא מקבל את המתח מהמצברים ברציפות, כל הזמן. מערכות אל-פסק מקוונות מספקות מתח "נקי יותר", אולם הן יקרות יותר ממערכות אל-פסק בכוננות.

כל מערכת אל-פסק (UPS) טובה זקוקה למנגנון כלשהו שיודיע למערכות המחוברות אליה כשיש הפסקת חשמל. בדרך כלל, זהו כבל טורי שמחובר מכניסת האל-פסק אל הכניסה טורית בשרת. כפי שמוצג בתרשים 16.4, מחשבי שרת כוללים בדרך כלל תוכנה שיכולה לקבל התראה ממערכת אל-פסק, כדי להזהיר משתמשים ברשת על הפסקת החשמל, לספק פרק זמן שבו המשתמשים יוכלו לסגור את הקבצים שלהם, וליזום כיבוי מסודר של המערכת. אם המתח חוזר לפני תחילת תהליך הכיבוי, מערכת האל-פסק תודיע לשרת שהמתח חזר.



***תרשים 16.4**: Windows NT כוללת שירות לוח בקרה לטיפול בהתראות ממערכות אל-פסק*



הערה: יש צורך בהתקן אל-פסק לא רק כדי להגן על שרתי הרשת, אלא גם עבור ציוד הקישוריות של הרשת כגון נתבים, גשרים ורכזות. אם שרתים מתחזקים חיבורי רשת פתוחים, התקני קישוריות עלולים להיות חיוניים לכיבוי נכון של השרת.

אחסון דיסק בעל Fault Tolerance

דרך אחת למניעת תקלות ברשת היא להשתמש במערכת אחסון עמידה בתקלות כדי לאחסן בה נתונים חיוניים. **מערכת עמידה בתקלות**, או **מערכת בעלת סיבולת תקלות** (fault-tolerant system) היא כזו, בה המערכת ממשיכה לתפקד גם כאשר רכיב כלשהו כושל. מערכות אחסון עמידות בתקלות עשויות להיות מבוססות לחלוטין על חומרה, או שהן יכולות להכיל מרכיב תוכנה. רוב מערכות הפעלת רשת כוללות יכולת כלשהי להשתמש באחסון על דיסק Fault Tolerance.

השיטה העיקרית לסיווג מערכות דיסק עמידות בתקלות היא בעזרת רמת **RAID** - **R**edundant **A**rrays of **I**nexpensive **D**isks. המונח RAID מגדיר מספר רמות של מערכות אחסון בדיסק, כפי שמוצג בטבלה 16.2.

טבלה 16.2: *רמות RAID*

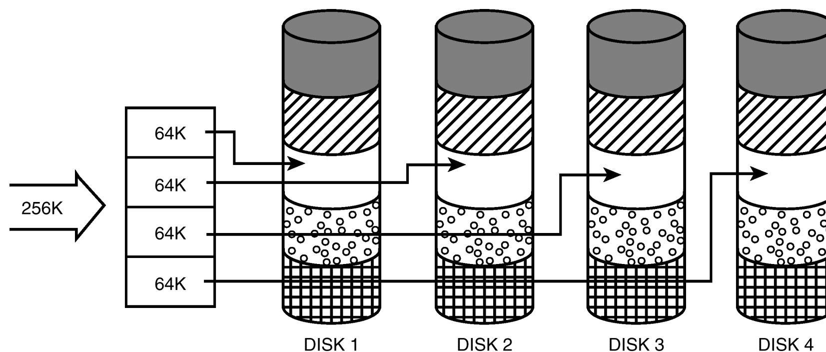
רמת RAID	תיאור
0	Disk striping by block
1	Disk Mirroring or Duplexing
2	Disk striping by bit with error correction codes
3	Disk striping by byte with parity information stored on single drive
4	Disk striping by block with parity information stored on single drive
5	Disk striping by block with parity information stored ocross Multiple drives

מערכות RAID משתמשות בעיקר בתהליך **חלוקה לרצועות דיסק** (disk striping) שבו נתונים "מחולקים" לרצועות ונכתבים במספר כונני דיסק. הנתונים יכולים להיות מועברים על ידי בקר דיסק פשוט אל כל כונן דיסק לפי בתים בודדים, או לפי גושים גדולים יותר. המגבלה היחידה לחלוקה לרצועות היא, שרוב מערכות ההפעלה לרשת אינן יכולות לאחסן את מחיצת המערכת (system partition), או את מחיצת האתחול שלהן (boot partition) במערכת רצועות דיסק.

בסביבות העבודה של מיקרוסופט, Windows NT תומכת ברמות RAID (0, 1, 5), באמצעות תוכנית שירות הנקראת Disk Administrator (**מנהל הדיסק**): רמה 0 (disk striping), 1 (disk mirroring), ו- 5 (disk striping with parity). רמה 5 נובעת מרמות 2,3 ו-4, ולכן היא מייצגת את היכולות העדכניות ביותר של אחסון בדיסק עמיד בתקלות. מיקרוסופט בחרה לתמוך ברמה 5 של RAID ולא ברמות 2 עד 4. Windows NT גם תומכת במנגנון מתקדם לאחסון בדיסק עמיד בתקלות הנקרא **sector sparing**.

Disk Striping - RAID 0

עבור שיפור ביצועי קריאה וכתיבה. ב-RAID רמה 0 (רצועות דיסק) גושי נתונים (גושים של 64K ב-Windows NT) נכתבים על פני מספר כונני דיסק, כפי שמוצג בתרשים 16.5. באמצעות פיזור הנתונים על פני מספר כוננים (2-32 דיסקים שונים) ניתן לשפר במידה משמעותית את ביצועי הקריאה והכתיבה, מכיון שנתונים נכתבים בו-זמנית במספר כוננים. בנוסף, ניתן להשתמש ביעילות במקום האחסון בכונן, מכיון ש**קבוצות רצועות** (striped sets) של נתונים יכולות להשתמש באזור מחיצה נוסף שאינו בשימוש במספר כוננים (ניתן להשיג זאת על בסיס התנאי הקיים עבור מערכת striped והוא שכל המחיצות (partitions) תהיינה ב**גודל אחיד**).



תרשים 16.5: *מערכות RAID 0 כותבות גושי נתונים במספר כוננים*

אולם, למרות הסיווג כחלק ממערכת RAID, RAID רמה 0 אינה מספקת כל עמידות בפני תקלות. אם אחד מכונני הדיסק כושל, הנתונים בכוננים האחרים לא יהיו שמישים, ואין כל דרך לשחזר נתונים מהדיסק שכשל. Windows NT מספקת תמיכה ב-RAID רמה 0, אך מומלץ להתייחס לרמת הגנה זו כאל **שיפור ביצועים**, ולא כברירה של ממש עבור Fault Tolerance.



רעיון מפתח

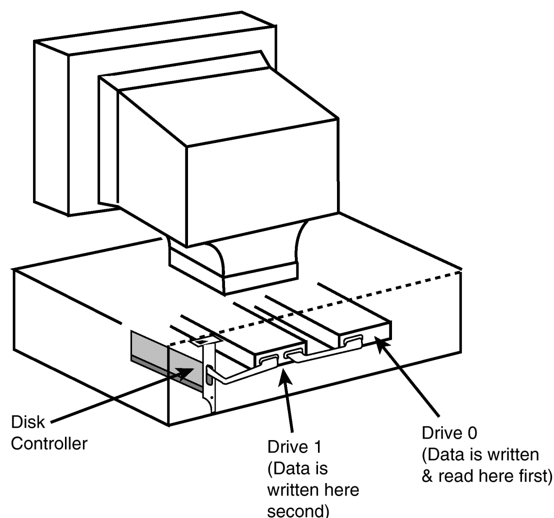
RAID רמה 0 משתמשת בחלוקה לרצועות לשיפור ביצועי הדיסק על ידי פיזור הנתונים במספר כוננים. RAID רמה 0 אינה מספקת רמה כלשהי של Fault Tolerance.

Disk Mirroring/Duplexing - RAID 1

עבור Fault tolerance, מספק את רמת הסיבולת הגבוהה ביותר. RAID רמה 1 משתמשת בטכניקה הנקראת **שיקוף דיסק** (disk mirroring), או **תמונת ראי**, ליצירת עותק של כונן דיסק אחד. למעשה, שני כונני הדיסק מחוברים לכרטיס בקר דיסק יחיד, כפי שמוצג בתרשים 16.6. היישומים שולחים נתונים לבקר הדיסק לכתיבתם בדיסק והבקר שולח את הנתונים לשני הכוננים. בדרך זו, כונן דיסק אחד הוא תמונת ראי של הדיסק השני. אם כונן דיסק אחד כושל, ניתן לשחזר נתונים מהכונן השני, כאילו דבר לא קרה.

שיקוף דיסק דורש שתי מחיצות (partitions) דיסק **בגודל זהה** שמוגדרות על שני כונני דיסק שונים. אין צורך להקצות את כל קיבולת כונן הדיסק לשימוש בשיקוף, אולם **השטח המוקצה חייב להיות זהה בשני הכוננים**. לביצועים אידיאליים, שני כונני הדיסק צריכים להיות מאותו יצרן, ו/או להיות בעלי מאפייני ביצוע זהים. שיקוף דיסק נפוץ כאשר רק כונן אחד הזקוק להגנה, או כשברצונך להגן על מחיצת המערכת (system partitions) או מחיצת האתחול (boot partitions).

החיסרון העיקרי של RAID רמה 1 הוא שתחזוקת מערכות חומרה כפולות עלולה להיות יקרה. כשיש שני כונני דיסק עם קיבולת אחסון של 1G בכל אחד, תוכל עדיין לאחסן רק 1GB של נתונים, מכיון שאתה משכפל את כל המידע.



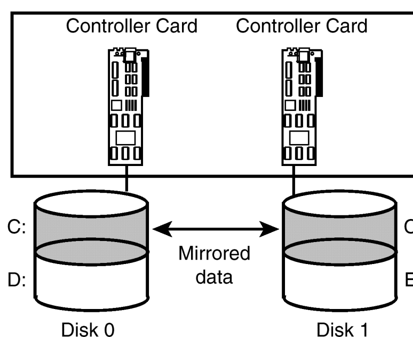
תרשים 16.6: *RAID רמה 1 מספק עמידות בפני תקלות באמצעות שיקוף דיסק*



רעיון מפתח

RAID רמה 1 משתמש ב**שיקוף דיסק** (disk mirroring) לכתיבת נתונים זהים לשני כונני דיסק נפרדים. במקרה של תקלה באחד הכוננים, משתמשים יכולים להמשיך ולהשתמש בכונן השני.

למרות ששיקוף דיסק מספק רמה גבוהה של עמידות בפני תקלות, עדיין קיימת נקודת כשל אחת בצורת כרטיס בקר (controller) דיסק יחיד. אם הכרטיס כושל מסיבה כלשהי, המשתמשים לא יוכלו לגשת לנתונים כלשהם באף לא אחד מהכוננים, עד להחלפת כרטיס בקר הדיסק. כדי למנוע בעיה זו, **שכפול דיסק** (disk duplexing), כפי שתראה בתרשים 16.7, מיישם שיקוף דיסק באמצעות כרטיס בקר דיסק נפרד לכל אחד מהכוננים. הנתונים לא רק מועתקים, אלא כעת במקרה שכרטיס בקר דיסק כושל, המשתמשים לא ירגישו בתקלה.



תרשים 16.7: *על ידי שימוש בשני כרטיסי בקר דיסק, שכפול דיסק מבטיח נגישות לנתונים גם אם כרטיס בקר דיסק אחד כושל*

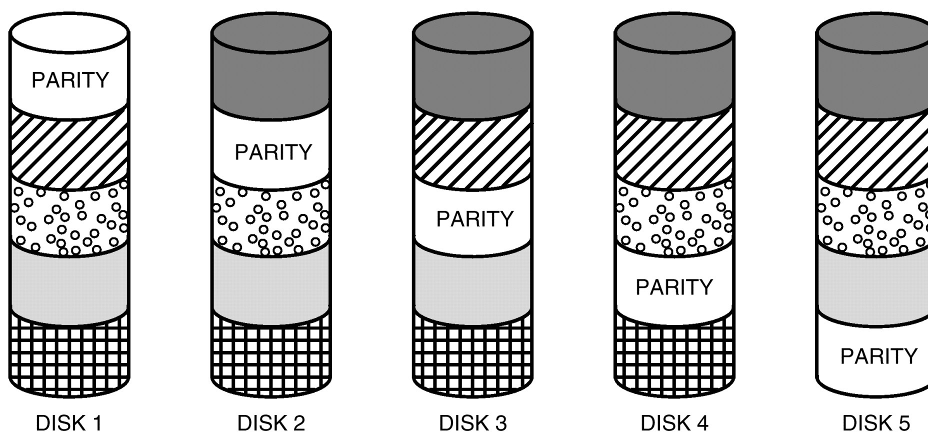


רעיון מפתח

שכפול דיסק (disk duplexing) היא גירסה של שיקוף דיסק, בה כל כונן דיסק משתמש בכרטיס בקר נפרד.

Disk Striping with Parity - RAID 5

עבור Fault tolerance, מספק רמת סיבולת גבוהה וחסכונית. בשעה ששיקוף דיסק (RAID Level 1) עלול להיות יקר, RAID רמה 5 מייעל את השימוש בשטחי אחסנה במספר כונני דיסק, תוך אספקת רמה גבוהה של Fault Tolerance. כפי שמוצג בתרשים 16.8, הנתונים מחולקים לרצועות על פני מספר דיסקים בתוספת נתוני בדיקת זוגיות (parity). כשכל רצועת נתונים נכתבת לדיסק, נוספים נתוני זוגיות באחד הגושים שנכתבים לדיסק. אם דיסק אחד כושל, הנתונים שנמצאים בו ניתנים לשחזור באמצעות הנתונים עצמם ונתוני הזוגיות שנמצאים בדיסקים שונים. Windows NT תומכת ב-RAID רמה 5 המשתמש ב-**3 עד 32 כונני דיסק**.



תרשים 16.8: *RAID Level 5 מפזר את הנתונים על פני מספר דיסקים וכולל נתוני זוגיות*

מימוש החלוקה לרצועות עם נתוני זוגיות עשויה להיות כדאית וכלכלית יותר משיקוף דיסק, מכיון שנעשה שימוש טוב יותר בשטחי האחסנה בדיסק על ידי חלוקה לרצועות עם נתוני זוגיות. לעומת שיקוף דיסק המאפשר שימוש רק ב-50 אחוזים מקיבולת הדיסק הכוללת, חלוקה לרצועות עם זוגיות מאפשרת שימוש כמעט בכל השטח של כונני הדיסק. נתוני זוגיות תופסים מעט מקום (1/n מהמקום הפנוי, כאשר n הוא מספר הכוננים בשימוש), והשאר פנוי לאחסון הנתונים עצמם.

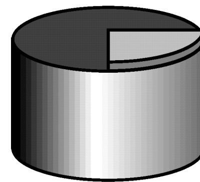


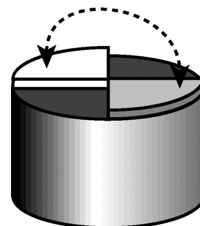
רעיון מפתח

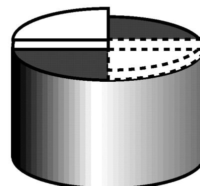
RAID Level 5 המוכר כ**חלוקה לרצועות עם זוגיות** (disk striping with parity), כותב נתונים ונתוני זוגיות על פני מספר דיסקים. אם דיסק כלשהו כושל, ניתן לשחזר את הנתונים מהנתונים ומנתוני הזוגיות השמורים בדיסקים האחרים.

Sector Sparing

עבור Fault Tolerance בסקטורים בודדים בסביבת Windows NT. בעוד שרמות RAID מתייחסות לכשל של כונני דיסק, מנגנון אחר לעמידות בפני תקלות מתייחס לתקלות בסקטורים בודדים בכונן הדיסק. באמצעות מנגנון הנקרא sector sparing (**חלופת סקטור**) או hot-fixing (תיקון-חם), בקר הדיסק ותוכנת דרייבר בעלת Fault Tolerance יכולים לזהות מתי נתונים נקראים מסקטור פגום, או עומדים להיכתב אל סקטור כזה. כפי שמוצג בתרשים 16.9, כאשר נתונים נמצאים בסקטור פגום, הם מועברים מייד לסקטור תקין והסקטור הפגום ממופה כדי שלא יהיה זמין עוד לנתונים.







תרשים 16.9: *sector sparing מעביר נתונים מסקטור פגום אל סקטור תקין*

Windows NT כוללת דרייבר עמיד בפני תקלות שיכול לתמוך ב- sector sparing בכונני **דיסק מסוג SCSI**. Windows NT גם כוללת תוכנית שירות המתריעה בפני מנהלי מערכת על סקטורים פגומים שהתגלו בדיסקים.



רעיון מפתח

sector sparing **(חלופת סקטור)** - מנגנון Fault Tolerance **שלפיו נתונים מועברים מסקטור פגום לסקטור תקין, והסקטור הפגום מוצא משימוש.**

תוכנית התאוששות מאסון

גם כל התוכניות הטובות למניעת תקלות ברשת עדיין אינן מגינות לחלוטין מפני אסונות שעלולים להתרחש. שרפות, שטפונות ורעידות אדמה עלולים לפגוע בבניין המשרדים שלך. גנבים עלולים לרוקן את מרכז המחשבים מתוכנו, והפסקות חשמל ארוכות עלולות להשאירך ללא יכולות רשת.

למרות שלא תוכל להתכונן לכל אסון, תוכנית מפורטת ומתוכננת היטב להתאוששות מאסון עשויה למנוע אובדן ארוך טווח של יכולת עבודה ברשת. תוכנית התאוששות מאסון צריכה להיות מסמך כתוב שיופץ לעובדים ויישמר הן באתר עצמו והן מחוץ לו. תוכנית ההתאוששות מאסון צריכה לעסוק בנושאים כגון אלה:

- ✯ היכן שמור התיעוד אודות תצורת הרשת?
- ✯ איזה נתונים מגובים ובאיזו תדירות? מה בנוגע למידע תצורת מערכת שאינו מגובה באופן סדיר?
- ✯ כיצד והיכן מאוחסנים גיבויים באתר? כמה מהר ניתן לשחזר, ועד כמה קל לשחזר אותם ובאיזו דרך?
- ✯ כיצד והיכן שמורים גיבויים שאינם באתר? כמה קל ניתן לשחזר אותם וכיצד?
- ✯ האם כל השרתים מחוברים למערכות UPS למקרה של נפילת מתח?
- ✯ איזה סוג של מערכות דיכוי וכיבוי אש מותקנות באזורי המחשבים?
- ✯ אם אתה מחובר לאינטרנט? איזה סידורים נעשו לניתוב של דואר נכנס, או תעבורת אינטרנט אחרת, אל אתר חלופי?
- ✯ מהם מספרי הטלפון של ספקי הרשת והטלקומוניקציה שלך? למי בארגון שלך (צוות מערכות מידע, מנהלים, וכדי) צריך להודיע במקרה אסון?
- ✯ איזה סוג של ביטוח עסקי יש לך? האם הוא יכסה אובדן נתונים?
- ✯ לאיזו רמת הכשרה זקוק הצוות שלך כדי להגיב במהירות וביעילות לתקלות ברשת?
- ✯ האם נתונים משוכפלים באתרים שונים, כדי שהפעילות תוכל להימשך באתר אחר במקרה של תקלה?
- ✯ האם יש לך יכולת להעביר פעילות רשת לאתר אחר?

תשובותיך לשאלות אלו ישתנו בהתאם לגודל הארגון, כמות הנתונים, היקף פעולות הרשת וחשיבות נתוני הרשת בפעילות היומיומית שלך. לאחר הקדשת מחשבה רבה, פיתוח תוכנית מקיפה להתאוששות מאסון עשויה לסייע לך למנוע אובדן נתונים הרה-אסון, אשר עלול להשפיע על התפקוד העסקי.

סיכום

כמנהל רשת, חלק מאחריותך הינו למנוע בעיות ברשת לפני שהן מתרחשות. הדבר כרוך בתיעוד נאות של הרשת, בקרה על ביצועי הרשת, גיבוי נתונים, אספקת מנגנונים למניעת כשל בציוד, ופיתוח תוכנית מקיפה להתאוששות מאסון.

בתיעוד הרשת יש לכלול מסמכים המתארים את רכיבי החומרה והתוכנה ואת תצורת הרשת. מידע כגון מספרי טלפון חשובים, יחסים עם ספקים, ופתרונות מוצלחים של בעיות בעבר, עשוי להגדיל במידה רבה את ערך התיעוד בעת ניסיון לאבחן תקלה.

בעת בקרה על ביצועי הרשת, תבלה את רוב זמנך בחיפוש אחר צווארי בקבוק בביצועי המערכת. צווארי בקבוק כוללים התקני רשת איטיים מדי, או שעמוסים מעבר ליכולתם בגלל רמת התעבורה ברשת. כלי שיכול לסייע לך הוא Performance Monitor (מנטר ביצועים) שנכלל ב-Windows NT. התקנים המשתמשים ב-SNMP (Simple Network Management Protocol) יכולים גם הם לסייע רבות. ב-SNMP, כל התקן מבוקר מכיל רכיב הרושם תעבורה וסטטיסטיקה אודות ההתקן. נתונים אלה נאספים על ידי תוכנית בקרה מרכזית שיכולה לנתח את הנתונים ולהציג גרפים ודוחות אודות מצב הרשת העדכני.

עם זאת, המנגנון החיוני ביותר למניעת תקלות ברשת הוא קרוב לוודאי מערכת גיבוי אמינה. מערכת גיבוי טובה כוללת את קביעת הנתונים שיש לגבות, נהלי הגיבוי, לוח הזמנים לגיבוי והאחראי לביצוע תהליך הגיבוי.

כדי למנוע תקלות ציוד, ניתן להשתמש במערכת אל-פסק - UPS (Uninterruptible Power Supply) ולמנוע נזק בעת נפילת מתח. לאחר שמערכת האל-פסק מחוברת לשקע החשמל שבקיר, מחברים אליה את ציוד המחשבים. כאשר יש הפסקת חשמל, היא תמשיך לספק מתח לציוד למשך פרק זמן מסוים. מערכות אל-פסק טובות יכולות להתריע בפני השרתים על הפסקת חשמל, כדי שיוכלו לכבות את עצמם בצורה מסודרת.

מנגנון נוסף להגנה בפני כשל בציוד הוא שימוש באחסון בעל Fault Tolerance בדיסקים. מערכות מסוג זה משתמשות בחלוקה לרצועות, שבה נתונים נשמרים על פני מספר כונני דיסק, שיקוף דיסק שבו נתונים נכתבים באופן זהה לשני כונני דיסק נפרדים, וגם שכפול דיסק שלפיו גם פועלים גם עם שני בקרי דיסק ולא רק בשני דיסקים. מערכות עמידות בפני תקלות מסווגות על פי רמות RAID (Redundant Arrays of Inexpensive Disks). בסביבות Microsoft מערכת Windows NT תומכת ב-RAID רמה 0 (disk striping), רמה 1 (disk mirroring) ורמה 5 (disk striping with parity).

לסיום, כמנהל רשת, עליך לפתח תוכנית מקיפה להתאוששות מאסון שתתייחס למה שקורה כשמתרחשת תקלה הרת-אסון כגון שריפה, הפסקת חשמל ארוכה, שיטפון, או אסון טבע אחר.

17

פתרון בעיות

עד כמה שתנסה למנוע בעיות ברשת, כאשר הן מתרחשות עליך להיות מוכן לאבחן את המערכת ולפתור את הבעיה. פרק זה יציג מתודולוגיה לזיהוי ולפתרון בעיות ברשת ואת הציוד המיוחד המשמש לאבחון בעיות אלו. עד סוף פרק זה תוכל:

- להסביר כיצד לנהוג בגישה מבנית לפתרון בעיות ברשת,
- לזהות ציוד שיכול לשמש לפתרון בעיות,
- לדעת היכן להשיג מידע נוסף לפתרון בעיות,
- לזהות טעויות נפוצות המתרחשות ברשת ולדעת לפתור אותן.

סקירה כללית של פתרון בעיות

פתרון בעיות רשת (network troubleshooting) אינו מדע, אלא אומנות שאתה מפתח במהלך שנות עבודתך ברשתות מחשבים. אם עבדת פרק זמן כלשהו עם מחשבים אישיים, כבר עומדים לרשותך מספר טיפים לפתרון בעיות במחשבים אישיים. לדוגמה, רוב משתמשי Windows יודעים שכאשר יישום אינו מגיב, ניתן להקיש Alt+Ctrl+Delete לסיום פעולת היישום ולאתחול מחדש של המחשב. רוב משתמשי מחשבים אישיים גם יודעים שכאשר יש ספק, הפעלה מחדש של המחשב פותרת במקרים רבים את הבעיה!

בדיוק כפי שפיתחת טיפים לפתרון בעיות ביישומי מחשבים אישיים, תוכל לפתח טיפים לפתרון בעיות רשת, ככל שתכיר אותן יותר. לפניך מספר טכניקות בסיסיות בעת פתרון בעיות רשת הקשורות למחשב אחד:

* **ודא תחילה שהתקלה אינה נובעת מטעות משתמש.** לפני שאתה מתעמק בפתרון הבעיה, רצוי שתחקור בעדינות את המשתמש המדווח על התקלה. ודא שהפעולה שהוא ניסה לבצע היא אכן כזו שניתן לבצע ברשת.
* **בדוק את החיבור הפיסי.** אחד הגורמים העיקריים לתקלות ברשת הוא התווך הפיסי. בדוק שכבל הרשת מחובר נכון למחשב, לרכזת, או למחשבים אחרים (תלוי בטופולוגיה). בדוק שבקצוות כבלים מחוברים נגדי סיום מתאימים ושכל התקני הקישוריות, כגון רכזות, מתפקדים היטב.
* **בדוק את כרטיס ממשק הרשת (NIC)**. רוב כרטיסי ממשק רשת יש שתי דיודות מאירות (LED) בגב הכרטיס. אחת מציינת שהכרטיס פועל והשנייה (הנקראת link light) מציינת שלמחשב יש חיבור פעיל לרשת.
* **הפעל מחדש את המחשבים**. כיבוי והפעלה מחדש של מחשב המשתמש יכול במקרים רבים לפתור תקלות ובעיות רשת.

אם שיטות אלו אינן פותרות את הבעיה שדווחה, או אם הבעיה קשורה למספר מחשבים, יש לנקוט בגישה מבנית יותר לפתרונה.

גישה מבנית

בעת התייחסות לבעיות רשת מורכבות, מיקרוסופט ממליצה על **גישה מבנית** (structured approach) לפתרון בעיות רשת. גישה זו כוללת חמישה שלבים:

1. הגדרת עדיפות הבעיה.
2. איסוף מידע לזיהוי התופעות.
3. פיתוח רשימה של גורמים אפשריים.
4. בדיקות לבידוד הגורם.
5. לימוד תוצאות הבדיקות לזיהוי פתרון.

הגדרת עדיפויות

הצעד הראשון בתהליך הוא לזהות את חומרת הבעיה. האם כל מחלקת המכירות אינה יכולה לעבוד מכיון ששרת בסיס הנתונים כָּשַל? האם הבעיה היא שמספר משתמשים אינם יכולים לשחק משחק כלשהו ברשת? או האם הבעיה היא שנשיא החברה אינו יכול לגשת לשרת הקבצים? המשימה הראשונה היא להקצות עדיפות לבעיה.

איסוף מידע

השלב הבא הוא איסוף מידע הן ממשתמשים והן מדוחות בקרת רשת. שאלות שיש לשאול משתמשים כוללות בין השאר:

- מהי בדיוק הבעיה שהם חווים? האם הרשת איטית מדי? האם יישום מסוים אינו פועל? האם המשתמש אינו יכול לראות משאב רשת מסוים?
- מתי החלה הבעיה? האם היא החלה עכשיו, או שהיא קיימת ומדווחת מזה זמן רב? האם הבעיה קבועה, או שמופיעה רק לעיתים?
- מה השתנה במחשב של המשתמש מאז שהחלה הבעיה? האם המשתמש התקין לאחרונה יישום כלשהו? האם שידרג את מערכת ההפעלה? האם המשתמש ניסה לתקן את הבעיה (ומה הוא עשה בפעולות תיקון אלו)?

לאחר איסוף נתונים מהמשתמשים המדווחים על הבעיה, יש לגשת לרשת ואז לשאול שאלות נוספות, ביניהן:

- האם הבעיה משפיעה על כל הרשת, או רק על מקטעים בודדים?
- מה השתנה ברשת מאז דיווח הבעיה? האם חלק מהשרתים הוגדרו מחדש? האם הוסף ציוד חדש או שהוסר ציוד ישן? האם הותקנו יישומים חדשים בשרתים?
- האם התוכנה או החומרה לבקרת הרשת מציגים מגמות כלשהן בתעבורת הרשת? האם מקטע כלשהו מציג תעבורה חריגה? האם ניתן לזהות צווארי בקבוק כלשהם ברשת?
- האם מישהו אחר בארגון מכיר בעיות דומות שהתרחשו ברשת בעבר?

לאחר הכנת רשימה מקיפה של תופעות שקרו ברשת, אתה מוכן להמשיך ולקבוע מה עשוי להיות הגורם לבעיה.

זיהוי גורמים אפשריים

הצעד הבא הוא הרכבת כל המידע שנאסף, וניסיון לקבוע מה עשוי להיות הגורם לבעיה. על סמך ניסיונך ברשת, הכן רשימת גורמי תקלה אפשריים. מה לדעתך לא תקין? השתמש במשאבים כדוגמת Microsoft TechNet לזיהוי בעיות אפשריות שתוכל להוסיף לרשימה זו. לאחר שתהיה בידך רשימת גורמי התקלות האפשריים, דרג אותם לפי סדר, מהגורם הסביר ביותר עד לגורם הפחות סביר.

בודד את הבעיה

לאחר שקבעת גורמים אפשריים, התחל בבדיקת הגורם הסביר ביותר. אם אתה חושד בחיבור הפיסי בין מחשב לרכזת, נסה להחליף את הכבל. אם אתה מאמין שכרטיס ממשק הרשת אינו תקין, החלף אותו בכרטיס חדש. אם אתה חושב שהגדרות TCP/IP אשמות, הגדר אותן מחדש.

במהלך שלב זה, מומלץ לבצע שינוי אחד בלבד בכל פעם. ודא שכל שינוי שאתה מבצע הינו אמין, ואל תיצור או תגרום לבעיות נוספות. לדוגמה, בעת החלפת כרטיס ממשק רשת, ודא שהכרטיס החלופי מתפקד היטב לפני הכנסתו למחשב.

חשוב שתנהל רישום של השינויים המבוצעים למערכת בתחום החומרה, התוכנה וההגדרות. בכל פעם שאתה מבצע שינוי, אתה עלול לגרום לבעיות נוספות. רישום הפעולות יאפשר לשחזר פעולות, אם יהיה צורך, עד לנקודת התחלה כלשהי.

לימוד התוצאות

לאחר כל בדיקה, בחן מה קורה וראה אם הבעיה תוקנה. אם כן, תעד את הבעיה ואת הדרך שבה פתרת אותה. אם לא, חזור לרשימת הגורמים האפשריים והמשך לבדוק אפשרויות נוספות.

כלים לפתרון בעיות

ככל שתעבוד ברשתות, תגלה שרוב הבעיות ברשת נובעות מבעיות בשכבה הפיסית. נתקים או קצרים בכבלים, כרטיסי ממשק רשת פגומים, חיבורים לקויים, ורשתות ללא **נגדי סיום** (terminators) מתאימים יכולים לגרום נזק ברשת. בעיות פיסיות יכולות לעיתים להיות הבעיות הקשות ביותר לאיתור. עם זאת, קיימים מספר כלים שיוכלו לסייע לך, ביניהם:

- DVM - digital volt meters (מדי מתח דיגיטליים),
- TDR - Time-domain reflectometers (מד החזר זמן-תחום),
- protocol analyzers (נַתָּחֵי פרוטוקולים),
- advanced cable testers (בוחני כבל מתקדמים),
- network monitors (מנטרי רשת),
- terminators (נגדי סיום).

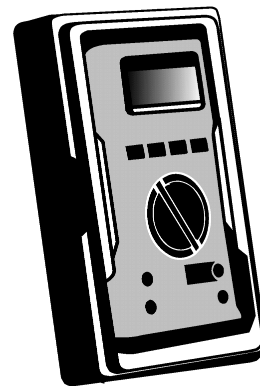


טיפ: ודא שאתה מבין את הכלים לפתרון בעיות, אולם הבחן במיוחד בין DVM, TDR ו-Protocol Analyzers.

מד מתח דיגיטלי - DVM

אחד מכלי המדידה האלקטרוניים הבסיסיים הקיימים כיום הוא **מד המתח הדיגיטלי - DVM** (digital volt meter) המוצג בתרשים 17.1. ניתן להשתמש ב-DVM למדידת המתח של סוללות או זרם חשמל ביתי, אולם ברישות משתמשים בו לבדיקת רצף (continuity testing). את מוליכי הבדיקה של המכשיר ניתן לחבר לכל אחד מקצוות הכבל ואז מועבר בכבל זרם נמוך. אם ה-DVM אינו מראה התנגדות, הזרם זורם בחופשיות ואין נתק בכבל. אך אם המכשיר מראה התנגדות, פירוש הדבר שיש נתק בכבל שאינו מאפשר מעבר זרם.

לחילופין, DVM יכול לבדוק קיום קצר על ידי חיבור מוליך אחד לליבה המרכזית ואת השני לשכבת הסיכוך. בחיבור זה, קיום זרם פירושו שבדרך כלשהי הליבה המרכזית והסיכוך נוגעים זה בזה ומקצרים את החיבור.



***תרשים 17.1:** מד מתח דיגיטלי יכול לשמש לבדיקת רציפות (Continuity).*

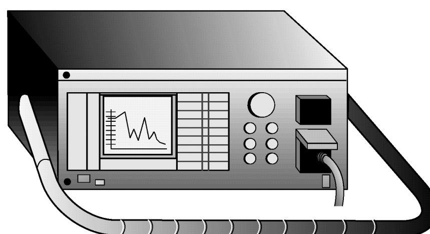


רעיון מפתח

DVM - מד מתח דיגיטלי - יכול לשמש לבדיקת נתק או קצר בכבל.

מד החזר זמן-תחום - TDR

כמו DVM גם מד החזר זמן-תחום, ה-TDR (time-domain reflectometer), שמוצג בתרשים 17.2, יכול לשמש לזיהוי נתק או קצר בכבל. אולם בעוד ש-DVM רק מזהה קיום נתק, TDR שולח אות חשמלי (דמוי סונר) בכבל, וכך הוא גם יכול לקבוע את מיקום הנתק או הקצר. כאשר האות נתקל בנתק או בקצר, הוא מוחזר לכיוון שממנו בא. TDR מודד את הזמן שנדרש לאות לחזור, ולפי סוג הכבל הנבדק **מעריך את מרחק הנתק** או הקצר ממכשיר המדידה. מכשירים טובים יכולים להעריך מרחק בדיוק של מספר מטרים מהנתק. קיימים מכשירים לבדיקת כבלים חשמליים וכבלי סיב-אופטי.



תרשים 17.2: *time-domain reflectometer (TDR) יכול להעריך היכן יש נתק בכבל*



רעיון מפתח

TDR - **מד החזר זמן-תחום** - משתמש באות דמוי סונר לקביעת מיקום נתק בכבל.

נַתָח פרוטוקולים (Protocol Analyzer)

בעוד ש-DVM ו-TDR בודקים רק את השלמות הפיסית של הכבל, **נתחי פרוטוקולים** (protocol analyzers) בודקים את המצב הכללי של הרשת על ידי בדיקת תעבורת הרשת ובחינת מנות. נתחי פרוטוקולים, הנקראים גם **נתחי רשת** (network analyzers), הם מוצרי חומרה, או שילובים שונים של חומרה ותוכנה. נתחי פרוטוקולים אוספים נתונים על ידי **בדיקת תוכן המנות** ויצירת תמונת פעילות של הרשת כולה.

כתוצאה מכך, ניתן להשתמש בנתחי פרוטוקולים לאיתור בעיות כגון אלו:

- צווארי בקבוק ברשת,
- כרטיסי ממשק רשת פגומים,
- יישומים סותרים,
- תעבורת רשת חריגה ממחשב מסוים,
- שגיאות חיבורים,
- רכיבי רשת לא תקינים.

בדרך כלל נתחי פרוטוקולים בחומרה כוללים time-domain reflectometer לזיהוי נתקים בשכבה הפיסית, אולם יכולתם בולטת **בניתוח מנות בשכבת קישור הנתונים, שכבת רשת התקשורת, ובשכבות עליונות** אחרות של מודל ייחוס OSI. יכולת זו מאפשרת לנתחי פרוטוקולים להתמקד במקטע רשת, או בפרוטוקול מסוים ולקבוע כיצד הם משפיעים על תעבורת הרשת הכוללת.

נתחי פרוטוקולים יכולים גם לשמש למעקב אחר ביצועי רשת, ובדרך כלל כוללים יכולת להפעיל התראות אם מתקיימים תנאי רשת מסוימים. לדוגמה, מנהל רשת ירצה אולי לדעת כאשר תעבורת הרשת מגיעה לרמת פעילות מסוימת, או כאשר רמות חריגות של מנות שידור לכל מציפות את המערכת (סערת שידור - Broadcast Storm).

דוגמאות נתחי פרוטוקולים כוללות: Sniffer של Network General, Network Advisor של Hewlett-Packard ו-LANalyzer של Novell. Windows NT Server 4.0 כולל גם את Network Monitor, שהינו נתח פרוטוקולים מבוסס תוכנה.



רעיון מפתח

נתח פרוטוקולים (protocol analyzer) הוא כלי עבודה בעל עוצמה לפיקוח על תעבורת רשת, לאיתור רכיבי רשת פגומים, ולניתוח ביצועי הרשת הכוללים.

בוחני כבל מתקדמים
(Advanced Cable Testers)

כמו DVM ו-TDR, גם **בוחני כבל** (cable testers) יכולים לבחון את הכבל ולמצוא נתקים וקצרים. אולם, בוחני כבל יכולים גם לקבוע מידע נוסף אודות הכבל כגון עכבה (impedance), התנגדות (resistance), הנחתה (attenuation) ומאפיינים פיסיים אחרים. בוחני כבל מתקדמים יכולים לעבור את השכבה הפיסית ולאסוף מידע אודות מניית מסגרות הודעה, התנגשויות מופרזות ושגיאות גודש.

לדוגמה, אם תחבר cabel tester לכבל Thinnet (RG-58A/U), הוא יראה עכבה של 50 אוהם. אם תחבר את בוחן הכבל לכבל ARCnet (RG-62), הוא יראה עכבה של 93 אוהם. עם ידע מסוים בערכי עכבה כאלה, טכנאי יכול להשתמש בבוחן כבל לאבחון בעיות.



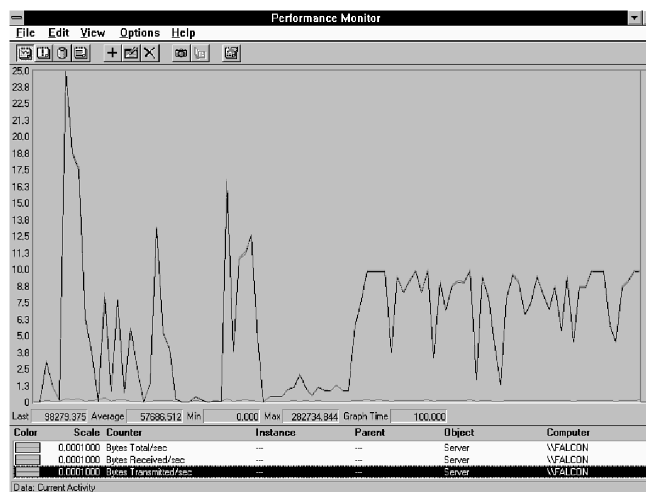
טיפ: דע שכאשר אתה מחבר בוחן כבל או אוהם-מטר (התקן לבדיקת עכבה בלבד) לכבל קואקסיאלי Thinnet, המכשיר צריך להראות 50 אוהם. באופן דומה, נגד סיום (terminator) Thinnet צריך להראות 50 אוהם. לעומת זאת, מחבר T או מחבר קנה (barrel connector) צריכים להראות 0 אוהם. הסיבה לכך היא ששני מחברים אלה מיועדים לחבר יחד מקטעי רשת, ואינם צריכים להוסיף התנגדות עצמית. בנוסף, אם הכבל יראה התנגדות אינסופית, זהו סימן שהאות נתקל בנתק בכבל.



הערה: DVM ו-TDR בודקים זרימה ואילו בוחן כבל בודק התנגדות, לכן הערך 00:Infinite ב-DVM וב-TDR מציג זרימה תקינה ואילו בבוחן הכבל מאפיין ערך זה בעיה.

מנטר רשת (Network Monitor)

מנטרי רשת (network monitors) הם תוכניות המשמשות למעקב ופיקוח על תעבורת הרשת. על ידי בחינת סוגי המנות, יכולים מנטרי הרשת לחולל דוחות וטבלאות אודות תעבורת המנות, שגיאות ותעבורת רשת כוללת. בעוד שפונקציות מנטרי רשת מסופקות על ידי נתחי פרוטוקולים שהוזכרו לעיל, תוכנת מנטר רשת בסיסית מסופקת עם רוב מערכות ההפעלה של מיקרוסופט (ראה תרשים 17.3). כפי שהוזכר בפרק 16, "מניעת תקלות ברשת", מעקב אחר ביצועי רשת להגדרת קו בסיס עבור הרשת עשויה לסייע בפתרון בעיות. מנטרי רשת פועלים בעיקר **משכבת קישור הנתונים של מודל OSI ומעלה אל השכבות הגבוהות יותר**.



תרשים 17.3: *Performance Monitor של Windows NT מספק תצוגה חזותית של תעבורת הרשת שהוא מודד*

נגד סיום (Terminator)

בעת אבחון בעיות כבלים ברשת המשתמשת בכבלים קואקסיאליים, TDR יכול להעריך את מיקום הנתק ולסייע באיתור הבעיה. אולם אם אין ברשותך TDR, נגד סיום (terminator) פשוט יוכל לספק מידה של סיוע. כפי שהוסבר בדיון אודות DVM, ניתן לחבר נגד סיום בקצה אחד של הכבל ולהשתמש ב-DVM למדידת רציפות הכבל.



תרשים 17.4: *נגד סיום (terminator)*

ניתן גם לנסות לאתר ידנית את הנתק על ידי שימוש בנגדי סיום. ברשת אפיק קואקסיאלית, מצא חיבור רשת, בערך במרכז הרשת. פרק את החיבור והצב נגד סיום בכל קצה כדי לפצל את הרשת לשני חלקים. אם יש רק נתק אחד, חלק אחד מהרשת אמור לתפקד כעת, בעוד החלק השני לא יתפקד. חזור על תהליך זה בחלק הרשת שאינו מתפקד והמשך לפצל לשניים את חלק הרשת הזה, עד לבידוד מקטע הכבל שבו יש נתק (זוכר את השיטה לתפיסת אריה במדבר?). תהליך זה אינו קל כמו שימוש ב-TDR, אולם יבצע את המשימה.



הערה: תהליך זה עלול להיות מסובך אם כל שרתי הרשת נמצאים במקטע רשת אחד, כאשר הרשת מפוצלת. אם זה המצב, עדיין ייתכן שתקשורת **אינה** מתרחשת במקטע האחר בגלל היעדר שרתים. ייתכן שתצטרך לפצל את הרשת כך שלפחות שרת אחד יהיה בכל מקטע.

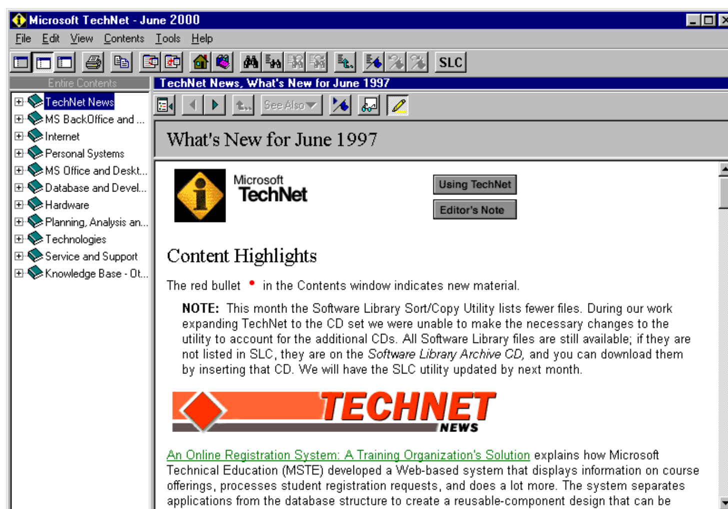
משאבים לפתרון בעיות

במהלך פתרון בעיות ברשת שלך, אתה עשוי להזדקק למשאבים נוספים. למשל, חברת Microsoft מאפשרת לך גישה למספר מקורות וביניהם :

- Microsoft TechNet (רשת מידע טכני של מיקרוסופט),
- Microsoft Knowledge Base (מאגר הידע של מיקרוסופט),
- Vendor Support Sites (אתרי תמיכת ספקים),
- Newsgroups (קבוצות דיון),
- Periodicals (כתבי עת).

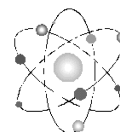
Microsoft TechNet

אם אתה עובד ברשתות המשתמשות במערכות הפעלה של מיקרוסופט, אחד המשאבים הטובים ביותר שתוכל להשתמש בהם הוא Technical Information Network - TechNet (רשת מידע טכני) של מיקרוסופט. כמנוי ל-TechNet, תקבל בכל חודש מערכת תקליטורים המכילים עושר עצום של מידע מוצרים, עדכוני תמיכה טכנית, דרייברים לתוכנות ומדריכים מקוונים. הממשק הקל-לשימוש, המוצג בתרשים 17.5, מאפשר לך להציג שאילתה לבסיס נתוני התמיכה הטכנית שעל התקליטור, בחיפושיך אחר תשובות לבעיות רישות.



תרשים 17.5: *TechNet, רשת המידע הטכני של מיקרוסופט מספקת דרך קלה לחיפוש פתרונות לבעיות רישות*

TechNet הוא משאב משתלם מאוד לסיוע באבחון בעיות רשת. תוכל להצטרף כמנוי ל-TechNet דרך חברת כלנית, בטלפון 03-6386363.



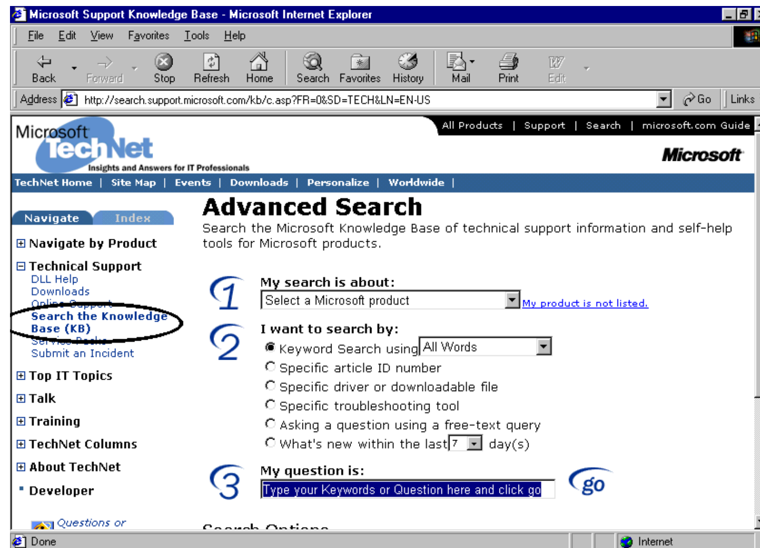
זה ה- Web

תוכל לקבל מידע נוסף אודות TechNet של מיקרוסופט באתר Web בכתובת

http://www.microsoft.com/technet/

Microsoft Technical Support

אם אין לך גישה ל-TechNet, תוכל לקבל רבים מהטיפים בנושאי תמיכה באמצעות Microsoft Technical Support המקוון ב-Web, כפי שתראה בתרשים 17.6.



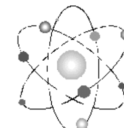
תרשים 17.6: *Technical Support המקוון של מיקרוסופט מספק דרך אחרת למציאת טיפים לתמיכה טכנית*

Vendor Support Sites

כיום, רוב הספקים של מוצרי רישות מספקים סוג כלשהו של תמיכה טכנית למוצריהם.

Newsgroups

אל תמעיט בערכן של **קבוצות דיון** בעת ניסיון למצוא את התשובה לבעיה. במקרים רבים, משלוח שאלה לקבוצת הדיון המתאימה עשוי להניב פתרון מהיר מאנשי מקצוע אחרים בתחום הרישות. בנוסף, מכיון שרוב כלי החיפוש הנפוצים ב-Web מספקים כיום יכולת לדפדף בקבוצות דיון, תוכל גם לבדוק אם מישהו כבר שאל (וקיבל תשובה) את השאלה שלך.



על ה- Web

http://www.dejanews.com. אתרי Web כמו DejaNews מתמחים בחיפוש בקבוצות דיון.

Periodicals

בקצב השינוי המהיר בתעשיית התקשורת, **כתבי עת** עשויים להיות דרך יעילה לעקוב אחר המגמות והטכנולוגיות החדשות ביותר ברישות מחשבים. קיימים מספר עיתונים שבועיים וחודשיים מצוינים המתייחסים לנושאי רישות, וביניהם: LAN Magazine, LAN Times, Communications Week, InfoWorld, ו- PC Week. רבים מהעיתונים מציעים מנויים חינם, אם תמלא שאלון ותתאים לסוג הכישורים שהם מחפשים. לרוב העיתונים הקשורים לתקשורת, גם יש אתרי Web שבהם מוצעות מהדורות מקוונות, מידע אודות מנויים, ובמקרים רבים פורומים ותחומי תמיכה טכנית.

בעיות נפוצות

הגישה המבנית לפתרון בעיות שהוזכרה קודם עשויה לסייע במציאת פתרונות לבעיות מורכבות. עם זאת, תמצא שחלק מהבעיות הנפוצות יותר ברשתות מחשבים הן:

- ✯ בעיות כבלים,
- ✯ כשל בהתקן קישוריות,
- ✯ כרטיסי ממשק רשת פגומים,
- ✯ גודש בתעבורת רשת,
- ✯ נושאי תצורת NIC (IRQ ו- I/O port),
- ✯ סערות שידור (broadcast storms),
- ✯ בעיות דרייבר רשת,
- ✯ יישומי רשת,
- ✯ הגדרות פרוטוקול רשת שגויות,
- ✯ חוסר התאמה בין פרוטוקולי רשת,
- ✯ תנודות מתח.

בעיות כבלים

בעיות רשת רבות ניתן לייחס לכבלים פגומים. ודא שהכבל מחובר כנדרש, וכי משתמשים בסוג הכבל הנכון. לדוגמה, ודא שאינך משתמש בטעות בכבל קואקסיאלי של טלוויזיה בכבלים (RG-59) ברשת Thinnet (RG-58A/U או C/U). בדוק שאתה משתמש באותו סוג של UTP ברחבי הרשת. ודא שאינך חורג מאורכי כבלים מומלצים. מכשירי DVM ו-TDR יכולים לסייע בזיהוי בעיות בכבלים.

כרטיסי ממשק רשת פגומים

בסעיף "סקירה כללית של פתרון בעיות" הסברנו שבמקרים רבים ניתן לקבוע אם כרטיס ממשק רשת מתפקד כנדרש על ידי הסתכלות בנורות שבגב הכרטיס. אולם, האם יש סתירת IRQ עם התקן אחר במחשב? האם המשתמש לא יכול לגשת לרשת לאחר שהתקין כרטיס קול במחשב שלו? אם הכל נראה כשורה ואתה משתמש ב-TCP/IP, תוכל להשתמש בפקודה PING כדי לבדוק אם ניתן לראות מחשבים אחרים קרובים. תוכל גם לשקול להשתמש בנַתָּח פרוטוקולים, כדי לקבוע אם מנות מהמחשב מגיעות אל הרשת.

בעיות תצורת NIC (IRQ, Base I/O port)

בדוק את הגדרות התצורה של כרטיס ממשק הרשת, כדי לוודא שאין סתירה ב-IRQ או בכתובת החיבור של יחידות (base I/O port) ביחס להתקני חומרה אחרים. ראה פרק 6, "תמסורת נתונים", בדבר רשימת הגדרות תצורה וסתירות אפשריות. אם יש סתירה, המעבד לא יוכל לתקשר עם כרטיס ממשק הרשת. נסה להשתמש בהגדרות שונות.

בעיות דרייבר רשת

בדוק וודא שימוש בדרייבר המתאים עבור כרטיס ממשק הרשת. באמצעות לוח בקרת הרשת, תוכל לנסות להסיר את ה**מתאם** (adapter) ולהתקין אותו מחדש. תהליך זה יכריח את מערכת ההפעלה להתקין מחדש את הדרייבר מהתווך המקורי. שים לב שהדבר **אינו** כרוך בהסרה פיסית של כרטיס הרשת (NIC). אתה רק מסיר אותו מלוח בקרת הרשת.

הגדרות פרוטוקול רשת שגויות

ודא שכל ההגדרות עבור פרוטוקול הרשת נכונות. אם אתה משתמש ב-TCP/IP, האם **מסכת רשת המשנה** (subnet mask) מוגדרת נכון? האם המחשב מוגדר עם שער ברירת המחדל (Default Gateway) הנכון? אם אתה משתמש ב-IPX/SPX, האם נבחר סוג המסגרת (Frame Type) הנכון?

חוסר התאמה בין פרוטוקולי רשת

אם מחשב מתפקד היטב, אולם אינו יכול לראות משאבי רשת מסוימים, ודא שהמחשב ומשאבי הרשת משתמשים באותו פרוטוקול רשת. לדוגמה, אם מחשב המשתמש רק ב-IPX/SPX ינסה לגשת למשאבים משותפים על שרת המפעיל רק TCP/IP, לא תהיה כל תקשורת. הוסף את הפרוטוקולים המתאימים לאחד המחשבים לפתרון הבעיה.

כשל בהתקן קישוריות (Connectivity)

אם מקטע (segment) אחד של רשת מתפקד היטב, אולם מקטע אחר לא עושה זאת, תוכל מייד לחשוד בהתקן המחבר את המקטע שנפגע. בדוק פעילות תקינה של רכזות. הדבר נשמע טיפשי, אולם כדאי לוודא שאף אחד לא ניתק בטעות מרכזיה פעילה ממקור המתח שלה. אם שני מקטעים פועלים אולם לא יכולים לראות זה את זה, בדוק את הגשר או הנתב המחברים בין שני מקטעי הרשת.

גודש בתעבורת רשת

נַתָּח פרוטוקולים (analyzer) או מנטר רשת (monitor) יכולים לדווח על רמות גבוהות מדי של תעבורת רשת. נתח פרוטוקולים טוב יכול לסייע בבידוד המקטעים היוצרים רמות גבוהות של תעבורת רשת. על פי מידע זה תוכל לקבל החלטות בדבר חלוקת הרשת באמצעות גשרים או נתבים, להפחתת התעבורה הכוללת. נתחי פרוטוקולים יכולים גם להצביע על צווארי בקבוק ברשת.

סערות שידור (Broadcast Storm)

תיתכן תקלה בהתקני רשת כדוגמת כרטיסי ממשק רשת ורכזות שתגרום ליצירת מספר חריג של מנות שידור לכל. **סערת שידור** (broadcast storm) מסוג זה יכולה להביא לרוויה ברשת ולהאט באופן משמעותי את התעבורה הרגילה. ניתן להשתמש בנתח פרוטוקולים לזיהוי התקן הרשת שאינו מתפקד ולהחליפו. בהנחה שאתה משתמש בפרוטוקולי רשת מנותבים, נתבים יכולים לספק מידה מסוימת של הגנה מפני סערות שידור, מכיון שהם משמיטים מנות שידור לכל (Broadcast Packets).

יישומי רשת

אם הרשת איטית מאוד, בדוק מהם היישומים שמשתמשים בהם. משחקי רשת נפוצים כגון Doom ו-Quake, למשל, יכולים לגרום להאטה ברשת. יישומי אינטרנט אחדים, כמו למשל שירות החדשות PointCast, יכולים להעמיס את משאבי הרשת עם עדכונים שוטפים. ככל שה-Web נפוצה יותר ומפותחים יישומים חדשים לשימוש בה, יישומי אינטרנט ידרשו רוחב פס בעל קיבולת גדולה יותר.

תנודות מתח

האם היו לאחרונה תנודות באספקת המתח? הפסקת חשמל, ואפילו למספר שניות, עלולה לגרום לתקלות בשרתי רשת ואף לתקלה נמשכת ברשת, אם השרת אינו חוזר לתפקוד תקין. התקן אל-פסק - UPS (uninterruptible power supply) הוא ההגנה הטובה ביותר נגד בעיה מסוג זה. שים לב שאפילו תנודות מתח קלות המתרחשות בתדירות גבוהה (אולם אינן ארוכות מספיק להפלת שרת), יכולות גם הן לגרום נזק לציוד רישות רגיש. UPS טוב צריך גם לספק הגנה מפני בעיות הנוצרות כתוצאה מתנודות מתח קלות.

סיכום

פתרון בעיות ברשת כרוך בתהליך איסוף מידע אודות הבעיה, בידוד הבעיה, ותיקון המצב. מיקרוסופט מתארת גישה בת חמישה שלבים לפתרון בעיות ברשת:

1. הגדרת עדיפות הבעיה - Problem's Priority.
2. איסוף מידע לזיהוי התופעות - Identify the Symptoms.
3. פיתוח רשימה של גורמים אפשריים - Possible Causes.
4. בדיקות לבידוד הגורם - Isolate the Cause.
5. לימוד תוצאות הבדיקות לזיהוי פתרון - Identify a Solution.

גישה מבנית כזו מאפשרת תהליך שיטתי כדי לזיהוי בעיות רשת ופתרונן.

לאיסוף מידע תוכל להיעזר במספר כלי אבחון. בשכבה הפיסית של מודל ייחוס OSI יכולים מכשירי **DVM** (digital volt meter) ומכשירי **TDR** (time domain reflectometer) לזהות נתק או קצר בכבל. על ידי שימוש באות חשמלי או אופטי דמוי סונר, TDR יכול להעריך את מיקום הנתק או הקצר בקו. **נתחי פרוטוקולים** (protocol analyzers) הם כלים מורכבים יותר, שכמו DVM ו-TDR יכולים לאבחן בעיות בשכבה הפיסית, אולם יכולים גם לבחון מנות ולפתור נושאים המתרחשים בשכבות קישור הנתונים ותקשורת הרשת. נתחי פרוטוקולים יכולים לזהות בעיות מורכבות יותר, כגון צווארי בקבוק בתעבורת הרשת, או מצב של יישומים סותרים.

בחיפוש אחר פתרונות תוכל להשתמש במשאבים רבים. TechNet של מיקרוסופט הוא משאב מבוסס תקליטור. תוכל להיות מנוי אליו, ולקבל מדי חודש מספר תקליטורים עם בסיס נתונים בר-חיפוש הכולל בעיות שגררו תמיכה טכנית, וגם מידע אודות מוצרים. מיקרוסופט גם מתחזקת בסיס ידע (Knowledge Base) ב-Web המספק מקום נוסף לחיפוש מידע. כיום רוב הספקים מאפשרים גישה למידע באמצעות ה-Web, וכך גם מספר רב של כתבי עת בנושא רישות.

לסיום, הבעיות הנפוצות ביותר המפריעות למשתמשי רשתות קשורות בדרך כלל בכבלים. בעיות נפוצות נוספות כוללות כרטיסי ממשק רשת פגומים, חוסר התאמה בין פרוטוקולים, ודרייברי רשת שאינם מתאימים.



טבלאות סיכום

פרק זה מכיל טבלאות המסכמות ערכים ופונקציות, המאפשרות מבט כולל על נתוני מידע בסביבת רשת. אוסף טבלאות זה אינו אמור להיות "במקום" הכתוב והמפורט בספר אלא "בנוסף".

החיבור הפיסי

	אורך מקסימלי	מהירות שידור	התקנה	רגישות להפרעות	עלות	מחבר
Fiber Optic	2000 מטר	100 Mbps–2 Gbps	קשה מאוד	אין	יקר מאוד	מיוחד
Thicknet RG-11 , RG-8	500 מטר	10 Mbps	קשה	נמוכה	יקר	AUI Transceiver Vampire-Tap
Thinnet RG-58	185 מטר	10 Mbps	קלה	בינונית	זול	BNC
STP	100 מטר	16-155 Mbps	בינונית	נמוכה	בינוני	Type A - 9 Pin
UTP 5 categories	100 מטר	10-100 Mbps	קלה	מאוד רגישה	זול ביותר	RJ-45
UTP Categories	**Category 1**	**Category 2**	**Category 3**	**Category 4**	**Category 5**	
		4 Mbps	10 Mbps דרישה מינימלית	16 Mbps	100 Mbps	

חיבור אלחוטי

(תדרי רדיו לשימוש לא מוסדר: 902-928 MHz, 2.4 GHz, 5.72-5.85 GHz)

	Frequency	מרחק שידור	מהירות שידור	התקנה	עלות	רגישות להפרעות	רגישות לאבטחה
רדיו							
Low-Power, Single Frequency	< GHz	10 מטר	1-10 Mbps	קלה	בינונית	רגיש	רגיש
High-Power , Single Frequency	< GHz	מעבר לאופק	1-10 Mbps	קשה דורש רשיון	בינונית עד גבוהה	רגיש	רגיש
Spread Spectrum	902-928 MHz	מיילים					
Direct Sequence			2-6 Mbps	קלה	בינונית	אין	אבטחה גבוהה
Frequency Hopping			< 1 Mbps	קשה	בינונית	אין	אבטחה מעולה
מיקרו-גל							
Terrestrial	21-23 GHz 4-6 GHz	מיילים	1-10 Mbps	בינונית	בינונית עד יקרה	מזג-אוויר	רגיש מאוד
Satellite	11-14 GHz	עולמי	1-10 Mbps	קשה מאוד	יקרה מאוד	מזג-אוויר והפרעות מגנטיות	רגיש מאוד
אינפרא-אדום							
Point to Point	100 GHz 1000 THz	Led - טווח עיניים לייזר – אלפי מטרים	100 Kbps -16 Mbps	בינונית	Led – זול לייזר – יקר מאוד	רגישות לאור	חסין
Broadcast	100 GHz 1000 THz	עשרות מטר	1 Mbps	קלה	זולה	רגישות לאור	רגיש מאוד

ארכיטקטורת הרשת

Ethernet	יתרון	חסרון	טופולוגיה	כבל / מחבר	גישה לתווך	אורך סגמנט	אורך רשת	בין צמתים	מספר סגמנטים	צמתים בסגמנט	מהירות	מפרט
10Base5	מרחקים- ארוכים.	עלות גבוהה. התקנה קשה.	BUS טרמינציה	Thicknet 50 Ohm RG-11 /8 AUI/DIX. Transceiver Vampire-Tap	CSMA / CD	500 מטר	2500 מטר	2.5 מטר	5 3 בפועל	100 300 ברשת כולה	10 Mbps	IEEE 802.3
10Base2	התקנה קלה. זול יחסית.	קשה לאיתור תקלות. מרחק מוגבל מספר צמתים קטן	BUS טרמינציה	Thinnet 50 Ohm RG-58 A/U RG-58 C/U BNC	CSMA / CD	185 מטר	925 מטר	0.5 מטר	5 3 בפועל	30 90 ברשת כולה	10 Mbps	IEEE 802.3
10BaseT	קל לאתר תקלות. התקנה קלה.	מרחק מוגבל.	STAR	UTP (3-5) RJ-45	CSMA / CD	100 מטר	----	2.5 מטר	1,024	1 1,024 ברשת כולה	10 Mbps	IEEE 802.3
10BaseF	מרחקים ארוכים מאוד. ביצועים	עלות גבוהה מאוד.	STAR	Fiber Optic מיוחד	CSMA / CD	2000 מטר	----	----	1,024	1 1,024 ברשת כולה	10 Mbps	IEEE 802.3
10BaseFL	Lan		STAR									
10BaseFP	Passive Hub		STAR									
10BaseFB	Backbone		Bus									

מעבר ממהירות 10Mbps ל- 100Mbps מחייב החלפת NIC, HUBS וכבל מתאים

100	יתרון	חסרון	טופולוגיה	כבל / מחבר	גישה לתווך	אורך סגמנט	אורך רשת	בין צמתים	מספר סגמנטים	צמתים בסגמנט	מהירות	מפרט
100BaseT	מהירות. קל לאיתור תקלות. התקנה קלה	עלות גבוהה. מגבלת מרחק.	STAR	UTP (3-5) סיב אופטי RJ-45	CSMA/CD		----	2.5 מטר	1,024	1 1,024 ברשת כולה.	100 Mbps	IEEE 802.3
TX				קטגוריה 5 2 זוגות		100 מטר						
T4				קטגוריה 3-5 4 זוגות		100 מטר						
FX				סיב אופטי		2000 מטר						
100VG-AnyLAN	מהירות שידור. קלה לאיתור תקלות. התקנה קלה	עלות גבוהה. טווח קצר.	STAR	UTP (3-4) UTP 5 .STP סיב אופטי RJ-45	Demand Priority	100 מטר ל UTP 3 150 מטר ל UTP 5 2000 מטר לסיב אופטי.	----	2.5 מטר	1,024	1 1,024 ברשת כולה.	100 Mbps	IEEE 802.12

Token Ring	יתרון	חסרון	טופולוגיה	כבל / מחבר	גישה לתווך	אורך סגמנט	אורך רשת	בין צמתים	מספר סגמנטים	מספר צמתים בסגמנט	מהירות	מפרט
	מהירות ויציבות	עלות גבוהה. קושי באיתור תקלות.	STAR	Type 1 , Type 3 , Category 5 RJ-45 Type A- (9 Pin)	Token-Passing	45 מטר ל UTP. 101 מטר ל STP.	----	2.5 מטר	33 מרכזיות	תלוי בסוג ה-MAU (8 – 16). מספר צמתים ברשת 77 עם UTP. ו 260 עם STP.	4-16 Mbps	IEEE 802.5 שימוש במגדלור איתות עבור תיקון עצמי

מפרטי IBM לסוגי כבל TP :

Type 1	Type 2	Type 3	Type 4	Type 5	Type 6	Type 7	Type 8	Type 9
STP 2 * 22Awg ליבת סיבים מלאה	STP 4*26Awg + 2*22Awg עבור העברת קול ונתונים בו זמנית	UTP 4*22Awg גרסה זולה של Type 1 מהירות נפגעת ל 4Mbps	-----	Fiber Optic עבור Backbone	STP 2*26Awg ליבת סיבים דקה. גמיש מ type 1 אך גם מוגבל במרחק	----	STP כמו Type 6 אך עם ציפוי שטוח להעברה מתחת לשטיחים	STP כמו Type 6 אך עם ציפוי Plenum להעברה בתקרות אקוסטיות

מפרט של IEEE לחיווט בסביבת Token-Ring:

UTP / TR = UTP מקטגוריה 5.

ARCnet	יתרון	חסרון	טופולוגיה	כבל/מחבר	גישה לתווך	אורך סגמנט	אורך רשת	בין צמתים	מספר סגמנטים	צמתים בסגמנט	מהירות	מפרט
	עלות נמוכה. קל להתקנה. יציבות.	איטיות. לא מתחבר עם ארכיטקטורות אחרות, כי אינו מבוסס על מספר צרוב ב NIC, אלא על SID המוגדר ע"י מנהל הרשת.	STAR (Active and Passive Hubs) BUS	Coaxe RG-62 A/U 93 Ohm. BNC ------ UTP RJ-45 ----- סיב אופטי	Token-Passing	600 מטר 121 מטר 3500 מטר	6000 מטר	משתנה	משתנה	עד 255 צמתים ברשת.	2.5 Mbps	ANSI 878.1
FDDI												
(Fiber Distributed Data Interface)	מהירות. טווח ארוך. יציבות. אבטחה.	עלות גבוהה מאוד. התקנה קשה.	RING Concentrators	סיב אופטי	Token-Passing	-----	100 ק"מ	----	---	מס צמתים ברשת 500	100 Mbps	ANSI X3T9.5



מילון מונחים עברי/אנגלי

במילון זה תמצא שני דברים :

1. המונחים באנגלית מסודרים לפי **A-Z** והתרגום שלהם לעברית.
2. המונחים השונים שמוסברים בספר מסודרים לפי **א-ת** והתרגום שלהם לאנגלית.
3. הסבר המונחים.

מילון זה אינו משמש כאינדקס. כדי למצוא את העמוד שבו מוסבר נושא מסוים - פנה לאינדקס המפורט.

אנגלי-עברי

Access	גישה
Access Methods	שיטות גישה
Access Permissions	הרשאות גישה
Access Privileges	זכויות הגישה
Active	אקטיבי
Active Hubs	רכזות אקטיביות
Active Monitor	תורן פעיל
Active Transmitter	משדר אקטיבי
Adapter	מתאם
Address Space	תחום כתובות IP
Addressing	הקצאת כתובות
Administering a Network	ניהול רשת
Administrative Privileges	זכויות ניהול
Administrator	מנהל
Advanced Cable Testers	בוחני כבל מתקדמים
Alerts	מתריעים
Analyser	נַתָּח פרוטוקולים
Antenna	אנטנה
Application	יישום
Application Programming Interface - API	ממשק תכנות יישומים
Application Server	שרת יישומים
Architecture	ארכיטקטורה
Area of Specialization - AOS	תחום התמחות
Asynchronous	אסינכרוניים
Attach	לצרף
Attenuation	דעיכת אות, ניחות, הנחתה
Attenuation	הנחתה, ניחות, דעיכת אות
Attenuation	ניחות, דעיכת אות, הנחתה
Audit Log	יומן ביקורת
Auditing	ביקורת
Auditing	פיקוח
Authenticated	יאומת

Authentication	בחינת אימות מרכזית
Backbone	אפיק שידרה
Backup	גיבוי מלא
Backup Log	יומן גיבוי
Backup System	מערכת גיבוי
Bands of Frequencies	תחומי תדרים
Bandwidth	רוחב פס
Bandwidth-On-Demand	רוחב פס-לפי-דרישה
Barrel Connector	מחבר קנה
Base Memory Address	כתובת בסיס זיכרון
Baseband	פס בסיס
Baseband Transmission	תמסורת פס-בסיס
Baseline	קו בסיס
Backup Domain Controller - BDC	בקר תחום גיבוי
Beaconing	איתות
Binding	קישור
Boot Partition	מחיצת האתחול
Bottleneck	צוואר בקבוק
Bouncing	החזרה
Bound	להתקשר
Braided	מעטה קלוע
Bridges	גשרים
Bridges	מגשרים
Bridging Table	טבלת גישור
Broadband	פס-רחב
Broadband Transmission	תמסורת פס-רחב
Broadcast	שידור לכל
Broadcast Infrared	שידור אינפרא-אדום
Broadcast Message	משדר הודעה
Broadcast packets	מנות שידור לכל
Broadcast Storm	סערת שידור
Brouters	נתבי-גשר
Browse	דפדף
Browser	דפדפן

Buffer .... חציצה
Bulletin Boards .... לוחות מודעות
Bus .... אפיק
Bus Mastering .... ניהול אפיק
Byte .... בית
Cable Testers .... בוחני כבל
Callback Capability .... יכולת חיוג חוזר
Casing .... מעטפת
Cell-Switching .... מיתוג תאים
Cellular .... סלולרי
Central Office - CO .... משרד מרכזי
Centralized Applications .... יישומים מרכזיים
Character Based .... מבוסס טקסט
Checkpoints .... נקודות ביקורת
Chips .... שבבים
Circuit .... מעגל
Circuit-Switched Connection .... חיבור ממותג-מעגלים
Circuit-switching .... מיתוג מעגלים
Cladding .... ציפוי הזכוכית
Classes .... סוגים
Client .... לקוח
Client License .... רשיון לקוחות
Client Operating Systems .... מערכות הפעלה של מחשבי לקוח
Client Software .... תוכנת לקוח
Client/Server .... שרת/לקוח
Client/server Applications .... יישומי שרת/לקוח
Client-Access-Licenses .... רשיונות-גישת-לקוח
Coaxial .... קואקסיאלי
Collective Document Creation .... יצירת מסמך משותפת
Collision .... התנגשות
Combination Networks .... רשתות משולבות
Communication/Message Server .... שרת תקשורת ודואר
Computer Networking .... רישות מחשבים
Concentrators .... רכזים

Conceptual Framework	מסגרת תפישתית
Conferences	ועידות
Congestion	גודש
Connection Equipment	ציוד חיבור
Connectionless	חסרי-קישור
Connectionless Broadcast	שידור חסר-קישור
Connectionless Datagram Service	שירות חסר-קישור
Connection-Oriented	מוכווני-קישור
Connectivity	קישוריות
Contention	תחרות
Continuity Testing	בדיקת רצף
Contributors	תורמים
Control Panel	לוח בקרה
Controller	כרטיס בקר
Copper	נחושת
Copper Wire	חוטי נחושת
Copy	העתקה
Core Exams	בחינות חובה
Credits	זכות
Daily Copy	העתק יומי
Data Access Language	שפת גישה לנתונים
Data Frames	מסגרות נתונים
Data Link	קישור נתונים
Data Transmission	תמסורת נתונים
Database Management Systems	מערכות ניהול מסדי נתונים
Database server	שרת בסיס נתונים
Datagrams	צרור נתונים
Decrypt	מפוענח
Dedicated Connection	חיבור ייעודי
Dedicated Leased Lines	קווים חכורים ייעודיים
Default Getway	שער ברירת המחדל
Delivery notifiCation Alerts	הודעות מסירה
Demand	דרישה
Demand Priority	עדיפות דרישה

Demarcation Point	נקודת תיחום
DEModulate	מפענח
Demultiplexes	מפרק
Description	תיאור
Detection	מזהים
Dial-up	חיבור בחיוג
Differential	דיפרנציאלי
Digital Volt Meters - DVM	מדי מתח דיגיטליים
Direct Memory Access - DMA	גישה ישירה לזיכרון
Directional Parabolic Antenna	אנטנה פרבולית כיוונית
Directory	ספריה
Directory Services	שירותי ספריה
Direct-Sequence Modulation	אפנון רציף
Disable	להשבית
Discard	נתבים משליכים
Discovery	גילוי
Discussion Bulletin Boards	לוחות מודעות לדיון
Disk Duplexing	שכפול דיסק
Disk File System	מערכת ניהול הקבצים
Disk Mirroring	שיקוף דיסק
Disk Striping	חלוקה לרצועות דיסק
Disk Striping With Parity	חלוקה לרצועות עם זוגיות
Dispersing	פיזור
Distance-Vector Algorithm	אלגוריתם וקטור-מרחק
Digital Network Architecture - DNA	ארכיטקטורת הרשת הדיגיטלית
Documentation	תיעוד
Domain	תחום
Domain Controller	בקר תחום
Domain Name	שם תחום
Domain Name System - DNS	מערכת שמות התחום
Drive Designators	מצייני כונן
Driver	דרייבר - מנהל הֶתקֵן
Driver Interfaces	ממשקי דרייבר
Drop cable	כבל סעף

Dual Attachment Concentrators .... רכזים עם חיבור כפול

Dual Attachment Stations - DAS .... תחנות בעלות חיבור כפול

Dual Inline Package Switch............ מתג DIP

Dynamic Routers............ נתבים דינמיים

Dynamic Routing............ ניתוב דינמי

Electromagnetic Frequency............ תדר אלקטרומגנטי

Electromagnetic Spectrum .... ספקטרום אלקטרומגנטי

Electronic Bulletin-Board .... לוח הודעות אלקטרוני

Electronic Mail............ דואר אלקטרוני

Electronic Mail Applications .... יישומי דואר אלקטרוני

E-Mail Systems............ מערכות דואר אלקטרוני

Encrypt............ מוצפן

Encryption .... הצפנה

Engine............ מנוע

Enterprise Networks............ רשתות תאגיד

Ethernet............ איתרנט

Executable Files .... קבצי הרצה

Fault Tolerance............ סיבולת לתקלות

Fault Tolerant............ סיבולת לתקלות

Fiber Distributed Data Interface - FDDI .... נתונים מבוזרים בסיב אופטי

Fiber-Optic .... סיב-אופטי

File Server............ שרת קבצים

File-Locking .... נעילת קובץ

Firewall............ קיר מגן

Forms............ טפסים

Forums .... פורומים

Forward .... גשרים מעבירים

Frame Relay .... ממסור מסגרות

Frame Type .... סוג מסגרת

Frames .... מסגרות

Frequency-Hopping .... דילוג בתדר

File Transfer Protocol - FTP............ פרוטוקול העברת הקבצים

Full-Time............ בלעדי וקבוע

Function............ תפקוד

Gateway	שער
Glass Fiber-Optics	סיבים אופטיים מזכוכית
Granting Dial-In Permission	הקצאת הרשאות חיוג
Graphical	גרפיקה
Group Accounts	חשבונות קבוצה
Group Accounts	חשבונות קבוצה
Group Discussions	דיונים קבוצתיים
Group Scheduling	תזמון קבוצתי
Groups	קבוצות
Groupware	יישום קבוצת עבודה
Groupware	קובצה
Guest Account	חשבון אורח
Hardware Addresses	כתובות חומרה
Help Desk	מרכז תמיכה
Home Directory	ספריית בית
Hops	קפיצות
Host	מארח
Host ID	קוד זיהוי מארח
Hot-Fixing	תיקון-חם
Hub	רַכֶּזֶת
Hybrid	רשתות היברידיות
Hypertext Links	קישורים
Impedance	עכבה
Impulse	פעימה
Incremental	תוספתי
Information Store	מחסן מידע
Infrared - IR	אינפרא-אדום
Integrated Circuit - IC	שבב מעגל משולב
Integrated Services Digital Network	רשת דיגיטלית של שירותים משולבים
Interconnected	מחובר יחד
Interference	הפרעה
Interlinked Cascading	רכזות המקושרות במידרוג
Intermediary Format	תצורת ביניים
Internal Publishing	הוצאה לאור פנימית

ארגון התקינה הבינלאומי - ISO .... International Standards Organization
ערכת פרוטוקול אינטרנט .... Internet Protocol Suite
הוצאה לאור באינטרנט .... Internet Publishing
שירותי אינטרנט .... Internet Services
מערכות אינטרנט .... Internet Systems
רשת משולבת .... Internetwork
שילוב רשתות .... Internetworking Device
פסיקה .... Interrupt
בקשת פסיקה .... Interrupt Request - IRQ
אינטראנט .... Intranet
ספקי שירותי אינטרנט .... Internet Service Providers - ISP
מגשר .... Jumper
שכבות .... Layers
גשרים לומדים .... Learning Bridges
חכור .... Leased
דיודה פולטת אור .... Light Emitting Diode - LED
אפיק ליניארי .... Linear Bus
קו ראייה .... Line-of-Sight
קישור .... Link
פרוטוקול בקרת קישור .... Link Control Protocol - LCP
אלגוריתם מצב-קישור .... Link-State Algorithm
רשת תקשורת מקומית .... Local Area Network - LAN
אפיק המקומי .... Local Bus
מעגל מקומי .... Local Loop
קבצי יומן .... Log Files
להתנתק .... Log out
בקרת קישור לוגי .... Logical Link Control - LLC
טבעת לוגית .... Logical Ring
תסריטי פקודות לכניסה .... Login Scripts
שירותי חוץ .... Long Distance
שרתי דואר .... Mail Servers
מחשבים גדולים .... Mainframe
בסיס נתוני ניהול .... Management Information Base
ממפה .... Map

תווך .... Media
בקרת גישה לתווך .... Media Access Control - MAC
כתובות חומרה .... Media Access Control Address - MAC
חבר .... Member
סריג .... Mesh
שירות טיפול בהודעות .... Message Handling Service
מחסן הודעות .... Message Store
סוכן העברת הודעה .... Message Transfer Agent - MTA
ממשקי תכנות יישומים להודעות .... Messaging Application Programming Interfaces
מערכות הודעות .... Messaging Systems
הודעות/קובצה .... Messaging/Groupware
רשת תקשורת מטרופוליטנית .... Metropolitan Area Network - MAN
ספריית מיקרוסופט שהורדה מהרשת .... Microsoft Download Library - MSDL
מיקרוגל .... Microwave
מודם .... Modem
מאפנן .... MOdulate
מנטר רשת .... Monitor
ניטור .... Monitoring
לטעון .... Mount
מרבבים .... Multiplexors
רב-נקודתי .... Multipoint
מגברים מרובי יציאות .... Multiport Repeaters
פענוח שמות .... Name Resolution
רשת .... Network
מתאם רשת .... Network Adapter
מנהל רשת .... Network Administrator
נתחי רשת .... Network Analyzers
כרטיס רשת .... Network Card
קוד זיהוי הרשת .... Network ID
כרטיס ממשק רשת .... Network Interface Card - NIC
תווך רשת .... Network Media
בקרת ביצועי הרשת .... Network Monitor
מנטרי רשת .... Network Monitors
מערכת הפעלת רשת .... Network Operating System

Network Performance Monitoring	ניטור ביצועי הרשת
Network Protocol	פרוטוקול רשת
Network Segment	מקטעי רשת
Network Stand-alone Applications	גרסאות רשת ליישומים עצמאיים
Network Troubleshooting	פתרון בעיות רשת
Network Version	גרסת רשת
Networking	רישות
Network-Only Applications	יישומי רשת-בלבד
News Servers	שרתי דיון
Newsgroups	קבוצות דיון
Next Station Identifier NID	קוד זיהוי התחנה הבא
Nodes	צמתים
Noise	רעש
Non-Routable	חסרי ניתוב
Objective Domain	תחום יעדים
Offline	לא מקוון
Onboard Microprocessor	מעבד על כרטיס
On-line	מקוון
Open Systems	מערכות פתוחות
Operating System	מערכת הפעלה
Optical Carrier	רמות תווך אופטי
Outages	נפילות
Packet	מנת נתונים
Packet Header	כותרת המנה
Packet Switching	מיתוג מנות
Packet-Filtering Routers	נתבים מסנני-מנות
Packets	מנות
Paging	איתור
Parallel	שידור מקבילי
Parallel Stream	זרם מקבילי
Parity	זוגיות
Partitions	מחיצות
Passive	פסיבי
Passive Hubs	רכזות פסיביות

Password-Protected Shares	שיתוף מאובטח-סיסמה
Passwords	סיסמאות
Patch	טלאי
Patch Cords	חוטי חיבור
Patch Panel	לוח חיבורים
Primary Domain Controller - PDC	בקר תחום ראשי
Public Data Networks - PDN	רשתות נתונים ציבוריות
Peer-to-Peer Network	רשת שוויונית
Peers	שוויונים
Performance Monitor	מנטר הביצועים
Periodicals	כתבי עת
Permission	הרשאות
Personal Address Book	ספר כתובות אישי
Personal Digital Assistants - PDA	יומנים אלקטרוניים אישיים
Physical	פיסית
Plenum	חללי אוורור
Plug and Play	הכנס-הפעל
Point to Point Protocol - PPP	פרוטוקול נקודה לנקודה
Point-to-Point Infrared	אינפרא-אדום נקודה-לנקודה
Polling	הזמנה לשידור
Polls	דוגֶמֶת
Port Access	כתובת כניסה
Post	שולח
Preamble	שדה הקדמה
Presentation	הצגה
Presentation	תצוגה
Primary Device	התקן עיקרי
Primary Ring	טבעת ראשית
Print Drivers	דרייברים למדפסת
Print Job	עבודת ההדפסה
Print Queue	תור הדפסה
Print Server	שרת הדפסה
Printing	הדפסה
Private Network	רשת פרטית

Propagation Delay .... השהיה
Protocol .... פרוטוקול
Protocol Analyzers.. נַתָּחֵי פרוטוקולים
Protocol Stack .... מחסנית פרוטוקול
Protocol Suites .... מערכות פרוטוקול
Proximity to the Backbone .... קירבה לאפיק השידרה
Proxy Servers.. שרתים מורשים
Public Folders .... תיקיות ציבוריות
Public Switched Telephone Network .... רשת טלפונים ציבורית ממותגת
Publick-Switched Network .... רשת ממותגת
Permanent Virtual Circuit - PVC .... מעגל מדומה קבוע
Queries.. שאילתות
Radio .... רדיו
Radio Frequency - RF .... תדר רדיו
Raw Ethernet .... אינטרנט גולמי
Receiver ....מקלט
Reconfiguring .... תצורה מחדש
Record-Locking .... נעילת רשומה
Redirector .... מנתב מחדש
Redirector .... תוכנת ניתוב
Reducing Congestion .... הפחתת הגודש
Redundancy .... יתירות
Redundant Arrays of Inexpensive Disks .... מערך יתיר של כוננים זולים
Reference model... מודל ייחוס
Relay Towers .... מגדלי ממסר
Reliable .... אמין
Repeaters ....מגברים
Request for Comments .... בקשות להערות
Resistance ....התנגדות
Return Receipts .... קבלות הֶחְזֵר
Right Click.. לחיצה ימנית
Ring.. טבעת
Ring In ....טבעת פנימה
Ring Out ....טבעת החוצה

Routable .... מנותבים

Router .... נתב

Routing Table .... טבלת ניתוב

Satellite Microwave .... מיקרוגל לוויני

Scheduling .... תזמון

Secondary Devices .... התקנים המשניים

Secondary Ring .... טבעת משנית

Sector Sparing .... חלופת סקטור

Security .... אבטחה

Security Identifier .... מזהה אבטחה

Security Policy .... מדיניות אבטחה

Segment .... מקטע

Sequencing .... רצף סדרתי

Serial .... שידור טורי

Serial Line Internet Protocol - SLIP .... פרוטוקול קו טורי לאינטרנט

Serial Stream .... זרם טורי

Server .... שרת

Server Based .... מבוסס שרת

Server Based Networks .... רשתות מבוססות שרת

Server Operating Systems .... מערכות הפעלת שרת

Server Software .... תוכנת שרת

Service .... שירות

Service Access Points - SAPs .... נקודות שירות גישה

Services .... שירותים

Session .... מושב

Setup Files .... קבצי הגדרות

Shared .... שיתוף

Shared Memory .... זיכרון משותף

Shared-File-sYstem Applications .... יישומי מערכת-שיתוף-קבצים

Share-Level Security .... אבטחה ברמת השיתוף

Shielded Twisted Pair - STP .... זוג שזור מסוכך

Shielding .... סיכוך

Security Identification Number - SID .... למספר זיהוי אבטחה

Single Attachment Concentrators .... רכזים עם חיבור בודד

Sync .... סיבית סנכרון
Synchronous .... סינכרוניים
Synchronous Transport Signals - STS .... אותות תמסורת סינכרוניים
System Partition.. מחיצת המערכת
Systems Management Server .... שרת ניהול מערכות
Technical Support .... תמיכה טכנית
Terminal .... מסוף
Terminal Session .... מושב מסוף
Terminator... נגד סיום
Terrestrial Microwave .... מיקרוגל קרקעי
Text Based .... מבוסס טקסט
The global Internet .... אינטרנט עולמית
Thicknet.. כבל עבה
Time Slots .... פרקי זמן
Time-Domain Reflectometers - TDR.................................. מד החזר זמן-תחום
Token.. אסימון
Token Passing.. העברת אסימון
Token-Ring.. טבעת אסימון
Top-Level Domains.. תחומים ברמה עליונה
Topology.. טופולוגיה
Tracks .... מסלולים
Transceiver.. מקלט/משדר
Translation Bridges .... גשרי תרגום
Transmitter .... משדר
Transparent Bridging .... גישור שקוף
Transport .... העברה
Transport/Delivery .... העברה/מסירה
Trunk .... כבל ראשי
Trusts Relationship .... אמון בין תחומים
Tuned... מכוונים
Type .... סוג
Uninterruptible Power Supply - UPS.................................. אל-פסק
Uninterruptible Power Supply - UPS.. התקן אל-פסק
Unshielded Twisted Pair - UTP .... זוג שזור לא-מסוכך

Upper Memory Address	כתובת זיכרון עליון
User Accounts	חשבונות משתמשים
User Agent - UA	סוכן דואר
User Name	שם משתמש
User Properties	מאפייני המשתמש
User-Level Security	אבטחה ברמת המשתמש
Users	משתמשים
Verified	מאומתים
Virtual Circuit	מעגל מדומה
Voice Grade	דרגת קול
Wide Area Network - WAN	רשת מרחבית
Web Pages	דפי Web
Web Server	שרת Web
Web Sites	אתרי Web
Wide Area Network - WAN	רשת תקשורת מרחבית
Wireless Bridge	גשר אלחוטי
Wireless Network Media	תווך רשת אלחוט
Wireless Technologies	טכנולוגיות אלחוט
Workflow Automation	אוטומציית זרימת העבודה
Workgroup appLications	יישומי קבוצת עבודה
Workgroups	קבוצות עבודה
Woven Steel Mesh	רשת פלדה ארוגה
Zone	אזור

עברי-אנגלי

אזור .... Zone
אבטחה .... Security
אבטחה ברמת המשתמש .... User-Level Security
אבטחה ברמת השיתוף .... Share-Level Security
אוטומציית זרימת העבודה .... Workflow Automation
אותות תמסורת סינכרוניים .... Synchronous Transport Signals - STS
אינטראנט .... Intranet
אינטרנט גולמי .... Raw Ethernet
אינטרנט עולמית .... the global Internet
אינפרא-אדום .... Infrared - IR
אינפרא-אדום נקודה-לנקודה .... Point-to-Point Infrared
איתור .... Paging
איתות .... Beaconing
איתרנט .... Ethernet
אלגוריתם וקטור-מרחק .... Distance-Vector Algorithm
אלגוריתם מצב-קישור .... link-State Algorithm
אל-פסק .... Uninterruptible Power Supply - UPS
אמון בין תחומים .... Trusts Relationship
אמין .... Reliable
אנטנה .... anTenna
אנטנה פרבולית כיוונית .... Directional Parabolic Antenna
אסימון .... Token
אסינכרוניים .... Asynchronous
אפיק .... Bus
אפיק המקומי .... local Bus
אפיק ליניארי .... Linear Bus
אפיק שידרה .... Backbone
אפנון רציף .... Direct-Sequence Modulation
אקטיבי .... Active
ארגון התקינה הבינלאומי - ISO .... International Standards Organization
ארכיטקטורה .... Architecture
ארכיטקטורת הרשת הדיגיטלית .... Digital Network Architecture - DNA

Web Sites	אתרי Web
Continuity Testing	בדיקת רצף
Cable Testers	בוחני כבל
Advanced Cable Testers	בוחני כבל מתקדמים
Core Exams	בחינות חובה
Authentication	בחינת אימות מרכזית
Auditing	ביקורת
Byte	בית
Full-Time	בלעדי וקבוע
Management Information Base	בסיס נתוני ניהול
Domain Controller	בקר תחום
Backup Domain Controller - BDC	בקר תחום גיבוי
Primary Domain Controller - PDC	בקר תחום ראשי
Network Monitor	בקרת ביצועי הרשת
Media Access Control - MAC	בקרת גישה לתווך
Logical Link Control - LLC	בקרת קישור לוגי
Request for Comments	בקשות להערות
Interrupt Request - IRQ	בקשת פסיקה
Congestion	גודש
Backup	גיבוי מלא
Discovery	גילוי
Access	גישה
Direct Memory Access - DMA	גישה ישירה לזיכרון
Structured Approach	גישה מבנית
Source-Route Bridging	גישור נתיב-מקור
Transparent Bridging	גישור שקוף
Network Stand-alone Applications	גרסאות רשת ליישומים עצמאיים
Network Version	גרסת רשת
Graphical	גרפיקה
Wireless Bridge	גשר אלחוטי
Translation Bridges	גשרי תרגום
Bridges	גשרים
Learning Bridges	גשרים לומדים
Forward	גשרים מעבירים

דואר אלקטרוני	Electronic Mail
דוגמת	Polls
דיודה פולטת אור	Light Emitting Diode - LED
דיונים קבוצתיים	Group Discussions
דילוג בתדר	Frequency-Hopping
דיפרנציאלי	Differential
דעיכת אות, ניחות, הנחתה	Attenuation
דפדף	Browse
דפדפן	Browser
דפי Web	Web Pages
דרגת קול	Voice Grade
דרייבר - מנהל התקן	Driver
דרייברים למדפסת	Print Drivers
דרישה	Demand
הדפסה	Printing
הדפסה ברקע	Spooling
הודעות מסירה	Delivery notifiCation Alerts
הודעות/קובצה	Messaging/Groupware
הוצאה לאור באינטרנט	Internet Publishing
הוצאה לאור פנימית	Internal Publishing
הזמנה לשידור	Polling
החזרה	Bouncing
הכנס-הפעל	Plug and Play
העברה	Transport
העברה/מסירה	Transport/Delivery
העברת אסימון	Token Passing
העתק יומי	Daily Copy
העתקה	Copy
הפחתת הגודש	Reducing Congestion
הפרעה	Interference
הצגה	Presentation
הצפנה	Encryption
הקצאת הרשאות חיוג	Granting Dial-In Permission
הקצאת כתובות	Addressing

הרשאות	Permission
הרשאות גישה	Access Permissions
השהיה	Propagation Delay
התנגדות	Resistance
התנגשות	Collision
התקן אל-פסק	Uninterruptible Power Supply - UPS
התקן עיקרי	Primary Device
התקנים המשניים	Secondary Devices
ועידות	Conferences
זוג שזור לא-מסוכך	Unshielded Twisted Pair - UTP
זוג שזור מסוכך	shielded Twisted Pair - STP
זוגיות	Parity
זיכרון משותף	Shared Memory
זכויות הגישה	Access Privileges
זכויות ניהול	Administrative Privileges
זכות	Credits
זרם טורי	Serial Stream
זרם מקבילי	Parallel Stream
חבר	Member
חד-תחומית	Single Domain
חוטי חיבור	Patch Cords
חוטי נחושת	Copper Wire
חיבור בחיוג	Dial-up
חיבור ייעודי	Dedicated Connection
חיבור ממותג-מעגלים	Circuit-Switched Connection
חכור	Leased
חלופת סקטור	Sector Sparing
חלוקה לרצועות דיסק	Disk Striping
חלוקה לרצועות עם זוגיות	Disk Striping With Parity
חללי אוורור	Plenum
חסרי ניתוב	Non-Routable
חסרי-קישור	Connectionless
חציצה	Buffer
חשבון אורח	Guest Account

חשבונות משתמשים ..... User Accounts
חשבונות קבוצה ..... Group Accounts
חשבונות קבוצה ..... Group Accounts
טבלת גישור ..... Bridging Table
טבלת ניתוב ..... Routing Table
טבעת ..... Ring
טבעת אסימון ..... Token-Ring
טבעת החוצה ..... Ring Out
טבעת משנית ..... Secondary Ring
טבעת ראשית ..... Primary Ring
טבעת לוגית ..... Logical Ring
טבעת פנימה ..... Ring In
טופולוגיה ..... Topology
טכנולוגיות אלחוט ..... Wireless Technologies
טלאי ..... Patch
טפסים ..... Forms
יאומת ..... Authenticated
יומן ביקורת ..... Audit Log
יומן גיבוי ..... Backup Log
יומנים אלקטרוניים אישיים ..... Personal Digital Assistants - PDA
יישום ..... Application
יישום קבוצת עבודה ..... Groupware
יישומי דואר אלקטרוני ..... Electronic Mail Applications
יישומי מערכת-שיתוף-קבצים ..... Shared-File-sYstem Applications
יישומי קבוצת עבודה ..... Workgroup appLications
יישומי רשת-בלבד ..... Network-Only Applications
יישומי שרת/לקוח ..... Client/server Applications
יישומים מרכזיים ..... Centralized Applications
יישומים עצמאיים ..... Stand-alone Applications
יכולת חיוג חוזר ..... Callback Capability
יצירת מסמך משותפת ..... Collective Document Creation
יתירות ..... Redundancy
כבל סעף ..... Drop cable
כבל עבה ..... Thicknet

כבל ראשי.. Trunk
כוכב .... Star
כוכב אפיק .... Star Bus
כוכב טבעת .... Star Ring
כוכב מחווט לטבעת.. Star-Wired Ring
כוננות .... Standby
כותרת המנה .... Packet Header
כרטיס בקר .... Controller
כרטיס ממשק רשת .... Network Interface Card - NIC
כרטיס רשת .... Network Card
כתבי עת.. Periodicals
כתובות חומרה .... Hardware Addresses
כתובות חומרה .... Media Access Control Address - MAC
כתובת בסיס זיכרון .... Base Memory Address
כתובת זיכרון עליון .... Upper Memory Address
כתובת כניסה .... Port Access
לא מקוון... Offline
להשבית .... Disable
להתנתק.. Log out
להתקשר... Bound
לוח בקרה .... Control Panel
לוח הודעות אלקטרוני .... Electronic Bulletin-Board
לוח חיבורים .... Patch Panel
לוחות מודעות .... Bulletin Boards
לוחות מודעות לדיון .... Discussion Bulletin Boards
לחיצה ימנית .... Right Click
לטעון.. Mount
ליבה מלאה... Solid Core
ליבת סיבים דקה .... Stranded Core
למספר זיהוי אבטחה .... Security Identification Number - SID
לצרף.. Attach
לקוח .... Client
מאומתים... Verified
מאפייני המשתמש .... User Properties

MOdulate .... מאפנן
Host .... מארח
Character Based .... מבוסס טקסט
Text Based .... מבוסס טקסט
Server Based .... מבוסס שרת
Repeaters .... מגברים
Multiport Repeaters .... מגברים מרובי יציאות
Relay Towers .... מגדלי ממסר
Jumper .... מגשר
Bridges .... מגשרים
Time-Domain Reflectometers - TDR .... מד החזר זמן-תחום
Digital Volt Meters - DVM .... מדי מתח דיגיטליים
Security Policy .... מדיניות אבטחה
Reference model .... מודל ייחוס
Modem .... מודם
Connection-Oriented .... מוכווני-קישור
Encrypt .... מוצפן
Session .... מושב
Terminal Session .... מושב מסוף
Security Identifier .... מזהה אבטחה
Detection .... מזהים
Barrel Connector .... מחבר קנה
Interconnected .... מחובר יחד
Partitions .... מחיצות
Boot Partition .... מחיצת האתחול
System Partition .... מחיצת המערכת
Message Store .... מחסן הודעות
Information Store .... מחסן מידע
Protocol Stack .... מחסנית פרוטוקול
Stand Alone .... מחשב בודד
Mainframe .... מחשבים גדולים
Microwave .... מיקרוגל
Satellite Microwave .... מיקרוגל לוויני
Terrestrial Microwave .... מיקרוגל קרקעי

מיתוג מנות .... Packet Switching

מיתוג מעגלים .... Circuit-switching

מיתוג תאים .... Cell-Switching

מכוונים .... Tuned

ממסור מסגרות .... Frame Relay

ממפה .... Map

ממשק תכנות יישומים .... Application Programming Interface - API

ממשקי דרייבר .... Driver Interfaces

ממשקי תכנות יישומים להודעות .... Messaging Application Programming Interfaces

מנהל .... Administrator

מנהל רשת .... Network Administrator

מנוע .... Engine

מנות .... Packets

מנות שידור לכל .... Broadcast packets

מנותבים .... Routable

מנטר הביצועים .... Performance Monitor

מנטר רשת .... Monitor

מנטרי רשת .... Network Monitors

מנת נתונים .... Packet

מנתב מחדש .... Redirector

מסגרות .... Frames

מסגרות נתונים .... Data Frames

מסגרת תפישתית .... Conceptual Framework

מסוף .... Terminal

מסכת רשת משנה .... Subnet Mask

מסלולים .... Tracks

מעבד על כרטיס .... Onboard Microprocessor

מעגל .... Circuit

מעגל מדומה .... Virtual Circuit

מעגל מדומה ממותג .... Switched Virtual Circuit - SVC

מעגל מדומה קבוע .... Permanent Virtual Circuit - PVC

מעגל מקומי .... Local Loop

מעטה קלוע .... Braided

מעטפת .... Casing

מערך יתיר של כוננים זולים	Redundant Arrays of Inexpensive Disks
מערכות אינטרנט	Internet Systems
מערכות דואר אלקטרוני	E-Mail Systems
מערכות הודעות	Messaging Systems
מערכות הפעלה של מחשבי לקוח	Client Operating Systems
מערכות הפעלת שרת	Server Operating Systems
מערכות ניהול מסדי נתונים	Database Management Systems
מערכות פרוטוקול	Protocol Suites
מערכות פתוחות	Open Systems
מערכת	Suite
מערכת גיבוי	Backup System
מערכת הפעלה	Operating System
מערכת הפעלת רשת	Network Operating System
מערכת ניהול הקבצים	disk File System
מערכת שמות התחום	Domain Name System - DNS
מפוענח	Decrypt
מפענח	DEModulate
מפרק	Demultiplexes
מצייני כונן	Drive Designators
מקוון	On-line
מקטע	Segment
מקטעי רשת	Network Segment
מקלט	Receiver
מקלט/משדר	Transceiver
מרבבים	Multiplexors
מרכז תמיכה	Help Desk
משדר	Transmitter
משדר אקטיבי	Active Transmitter
משדר הודעה	Broadcast Message
משרד מרכזי	Central Office - CO
משתמשים	Users
מתאם	Adapter
מתאם רשת	Network Adapter
מתג DIP	Dual Inline Package Switch

מתריעים .... Alerts
נגד סיום .... Terminator
נחושת .... Copper
הנחתה, ניחות, דעיכת אות .... Attenuation
ניהול אפיק .... Bus Mastering
ניהול רשת .... Administering a Network
ניחות, דעיכת אות, הנחתה .... Attenuation
ניטור .... Monitoring
ניטור ביצועי הרשת .... Network Performance Monitoring
ניתוב דינמי .... Dynamic Routing
ניתוב סטטי .... Static Routing
נעילת קובץ .... File-Locking
נעילת רשומה .... Record-Locking
נפילות .... Outages
נקודות ביקורת .... Checkpoints
נקודות שירות גישה .... Service Access Points - SAPs
נקודת תיחום .... Demarcation Point
נתב .... Router
נתבי-גשר .... Brouters
נתבים דינמיים .... Dynamic Routers
נתבים מסנני-מנות .... Packet-Filtering Routers
נתבים משליכים .... Discard
נתבים סטטיים .... Static Routers
נתונים מבוזרים בסיב אופטי .... Fiber Distributed Data Interface - FDDI
נתח פרוטוקולים .... Analyser
נתחי פרוטוקולים .... Protocol Analyzers
נתחי רשת .... Network Analyzers
נתיב-מקור .... Source-Route
סוג .... Type
סוג מסגרת .... Frame Type
סוגים .... Classes
סוכן דואר .... User Agent - UA
סוכן העברת הודעה .... Message Transfer Agent - MTA
סוכני תוכנה .... Software Agents

סיב-אופטי	Fiber-Optic
סיבולת לתקלות	Fault Tolerance
סיבולת לתקלות	Fault Tolerant
סיבים אופטיים מזכוכית	Glass Fiber-Optics
סיבית התחלה	Start Bit
סיבית סיום	Stop Bit
סיבית סנכרון	Sync
סיכוך	Shielding
סינכרוניים	Synchronous
סיסמאות	Passwords
סלולרי	Cellular
סערת שידור	Broadcast Storm
ספקטרום אלקטרומגנטי	Electromagnetic Spectrum
ספקטרום פרוש	Spread Spectrum
ספקי שירותי אינטרנט	Internet Service Providers - ISP
ספר כתובות אישי	Personal Address Book
ספריה	Directory
ספריית בית	Home Directory
ספריית מיקרוסופט שהורדה מהרשת	Microsoft Download Library - MSDL
סריג	Mesh
עבודת ההדפסה	Print Job
עדיפות דרישה	Demand Priority
עכבה	Impedance
ערכת פרוטוקול אינטרנט	Internet Protocol Suite
פורומים	Forums
פיזור	Dispersing
פיסית	Physical
פיקוח	Auditing
פס בסיס	Baseband
פסיבי	Passive
פסיקה	Interrupt
פס-רחב	Broadband
פעימה	Impulse
פענוח שמות	Name Resolution

פרוטוקול	Protocol
פרוטוקול בקרת קישור	Link Control Protocol - LCP
פרוטוקול העברת הקבצים	File Transfer Protocol - FTP
פרוטוקול נקודה לנקודה	Point to Point Protocol - PPP
פרוטוקול קו טורי לאינטרנט	Serial Line Internet Protocol - SLIP
פרוטוקול רשת	Network Protocol
פרקי זמן	Time Slots
פתרון בעיות רשת	Network Troubleshooting
צוואר בקבוק	Bottleneck
ציוד חיבור	Connection Equipment
ציפוי הזכוכית	Cladding
צמתים	Nodes
צרור נתונים	Datagrams
קבוצות	Groups
קבוצות דיון	Newsgroups
קבוצות עבודה	Workgroups
קבוצות רצועות	Striped Sets
קבלות החזר	Return Receipts
קבצי הגדרות	Setup Files
קבצי הרצה	Executable Files
קבצי יומן	Log Files
קו בסיס	Baseline
קו ראייה	Line-of-Sight
קואקסיאלי	Coaxial
קובצה	Groupware
קוד זיהוי הרשת	Network ID
קוד זיהוי התחנה	Station Identifier - SID
קוד זיהוי התחנה הבא	Next Station Identifier NID
קוד זיהוי מארח	Host ID
קווים חכורים ייעודיים	Dedicated Leased Lines
קיר מגן	Firewall
קירבה לאפיק השידרה	Proximity to the Backbone
קישור	Binding
קישור	Link

קישור נתונים ... Data Link

קישוריות ... Connectivity

קישורים ... Hypertext Links

קפיצות ... Hops

רב-נקודתי ... Multipoint

רדיו ... Radio

רוחב פס ... Bandwidth

רוחב פס-לפי-דרישה ... Bandwidth-On-Demand

רישוי אתר ... Site Licensing

רישות ... Networking

רישות מחשבים ... Computer Networking

רכזות אקטיביות ... Active Hubs

רכזות המקושרות במידרוג ... Interlinked Cascading

רכזות פסיביות ... Passive Hubs

רכזים ... Concentrators

רכזים עם חיבור בודד ... Single Attachment Concentrators

רכזים עם חיבור כפול ... Dual Attachment Concentrators

רכזת ... Hub

רמות תווך אופטי ... Optical Carrier

רעש ... Noise

רצף סדרתי ... Sequencing

רשיון לקוחות ... Client License

רשיונות-גישת-לקוח ... Client-Access-Licenses

רשת ... Network

רשת אופטית סינכרונית ... Synchronous Optical Network - SONET

רשת דיגיטלית של שירותים משולבים ... Integrated Services Digital Network

רשת טלפונים ציבורית ממותגת ... Public Switched Telephone Network

רשת ממותגת ... Publick-Switched Network

רשת מרחבית ... Wide Area Network - WAN

רשת משולבת ... Internetwork

רשת משנה ... Subnetwork

רשת פלדה ארוגה ... Woven Steel Mesh

רשת פרטית ... Private Network

רשת שוויונית ... Peer-to-Peer Network

רשת תקשורת מטרופוליטנית .... Metropolitan Area Network - MAN

רשת תקשורת מקומית .... Local Area Network - LAN

רשת תקשורת מרחבית .... Wide Area Network - WAN

רשתות היברידיות .... Hybrid

רשתות מבוססות שרת .... Server Based Networks

רשתות ממותגות .... Switched Networks

רשתות משולבות .... Combination Networks

רשתות נתונים ציבוריות .... Public Data Networks - PDN

רשתות תאגיד .... Enterprise Networks

שאילתות .... Queries

שבב מעגל משולב .... Integrated Circuit - IC

שבבים .... Chips

שדה הקדמה .... Preamble

שדה התחלה .... Start Frame Delimiter - SFD

שוויונים .... Peers

שולח .... Post

שידור אינפרא-אדום .... Broadcast Infrared

שידור חסר-קישור .... Connectionless Broadcast

שידור טורי .... Serial

שידור לכל .... Broadcast

שידור מקבילי .... Parallel

שיטות גישה .... Access Methods

שילוב רשתות .... Internetworking Device

שיקוף דיסק .... Disk Mirroring

שירות .... Service

שירות חסר-קישור .... Connectionless Datagram Service

שירות טיפול בהודעות .... Message Handling Service

שירות נתונים ממותג במהירויות גבוהות .... Switched Multi-megabit Data Service

שירותי אינטרנט .... Internet Services

שירותי חוץ .... Long Distance

שירותי ספריה .... Directory Services

שירותים .... Services

שיתוף .... Shared

שיתוף מאובטח-סיסמה .... Password-Protected Shares

שכבות	Layers
שכפול דיסק	Disk Duplexing
שם משתמש	User Name
שם תחום	Domain Name
שער	Gateway
שער ברירת המחדל	Defaolt Getway
שפת גישה לנתונים	Data Access Language
שרת	Server
שרת Web	Web Server
שרת בסיס נתונים	Database server
שרת הדפסה	Print Server
שרת יישומים	Application Server
שרת ניהול מערכות	Systems Management Server
שרת קבצים	File Server
שרת תקשורת ודואר	Communication/Message Server
שרת/לקוח	Client/Server
שרתי דואר	Mail Servers
שרתי דיון	News Servers
שרתים מורשים	Proxy Servers
תדר אלקטרומגנטי	Electromagnetic Frequency
תדר רדיו	Radio Frequency - RF
תווך	Media
תווך רשת	Network Media
תווך רשת אלחוט	Wireless Network Media
תוכנית הדפסה ברקע	Spooler
תוכנת לקוח	Client Software
תוכנת ניתוב	Redirector
תוכנת שרת	Server Software
תוספתי	Incremental
תור הדפסה	Print Queue
תורמים	Contributors
תורן בהמתנה	Standby Monitors
תורן פעיל	Active Monitor
תזמון	Scheduling

תזמון קבוצתי	Group Scheduling
תחום	Domain
תחום התמחות	Area of Specialization - AOS
תחום יעדים	Objective Domain
תחום כתובות IP	Address Space
תחומי תדרים	Bands of Frequencies
תחומים ברמה עליונה	Top-Level Domains
תחנות בעלות חיבור יחיד	Single Attachment Stations - SAS
תחנות בעלות חיבור כפול	Dual Attachment Stations - DAS
תחרות	Contention
תיאור	Description
תיעוד	Documentation
תיקון-חם	Hot-Fixing
תיקיות ציבוריות	Public Folders
תמיכה טכנית	Technical Support
תמסורת נתונים	Data Transmission
תמסורת פס-בסיס	Baseband Transmission
תמסורת פס-רחב	Broadband Transmission
תסריטי פקודות לכניסה	Login Scripts
תפקוד	Function
תצוגה	Presentation
תצורה מחדש	Reconfiguring
תצורת ביניים	Intermediary Format

הסבר המונחים

10Base2 An Ethernet network using Thinnet (50 ohm, 0.2 inch diameter) RG-58 A/U, or RG-58 C/U coaxial cable.

10Base5 An Ethernet network on Thicknet (50 ohm, 0.4 inch diameter) coaxial cable.

10BaseT An Ethernet network over Unshielded Twisted-Pair (UTP) cable using RJ-45 connectors.

10BaseF An Ethernet network using fiber-optic cable.

100BaseT Also referred to as Fast Ethernet or 100BaseX, a 100Mbps Ethernet network that can be subdivided into three categories: 100BaseTX, 100BaseT4, and 100BaseFX.

100VG-AnyLAN Originally developed by Hewlett-Packard and AT&T, provides speeds up to 100Mbps and uses the demand priority media access method rather than CSMA/CD.

A

ACK An acknowledgement signal.

acknowledgement In connection-oriented communication, the process used to guarantee reliable message delivery.

active monitor A node on a Token-Ring network that periodically sends out a signal to check that the network is free of errors. Usually the first computer to come online on a network.

active transmitter Transceiver unit that amplifies the signal before retransmitting the signal.

Advanced Program-to-Program Communications (APPC) A Session Layer protocol used with IBM SNA-based networks.

Advanced Research Projects Agency (ARPA) The agency responsible for the formation of the forerunner of the Internet. See DARPA.

AFP See AppleTalk Filing Protocol.

American National Standards Institute (ANSI) A standards-making organization based in the United States of America.

American Standard Code for Information Interchange (ASCII) A scheme that assigns letters, punctuation marks, and so on to specific numeric values. The standardization of ASCII enabled computers and computer programs to exchange data.

American Wire Gauge (AWG) The standards by which cables are defined based on specified wire diameters. AWG numbers are inversely assigned to diameters, meaning that larger AWG numbers indicate smaller diameters.

analog A signal with an infinite number of states, rather than just 1's and 0's. Voice, telephone, and television are examples of analog signals.

ANSI See American National Standards Institute.

ANSI character set An 8-bit character set used by Microsoft Windows that enables you to represent up to 256 characters (0–255) using your keyboard. The ASCII character set is a subset of the ANSI set. See American National Standards Institute.

API See application programming interface.

APPC See Advanced Program-to-Program Communications.

AppleTalk A simple, easy-to-use network architecture used by Apple Macintosh computers and included as part of the Macintosh operating system.

AppleTalk Filing Protocol (AFP) The AppleTalk protocol describing how files are stored and shared within an AppleTalk network. Operates in Presentation and Application Layers of the OSI model.

AppleTalk Phase 1 The original AppleTalk implementation where up to 32 computers could be connected on a network and only LocalTalk cabling was supported. With the use of hubs, the overall network could increase to 254 computers.

AppleTalk Phase 2 Introduced in 1989, allows the use of AppleTalk network protocols on top of Ethernet (EtherTalk) and Token-Ring (TokenTalk) architectures. Supports up to 16 million network nodes.

application A computer program that is designed to do some specific type of work—for example, a word processor, spreadsheet, database, game, or other application. An application is different from a utility which performs some type of maintenance (such as formatting a disk).

Application Layer The top layer of the OSI Reference Model that is primarily concerned with the interaction of the user with the computer. Services at this level support user applications such as electronic mail, database queries, network printing, and file transfer.

application programming interface (API) A list of supported functions that allow the programmers to interact with the network. Windows 95 supports the MS-DOS API, Windows API, and Win32 API. If a function is a member of the API, it is said to be a supported, or documented, function. Functions that make up Windows but are not part of the API are referred to as undocumented functions.

application server A file server on a network dedicated to providing access to applications.

archiving See backup.

ARCnet See Attached Resource Computer Network.

ARCnet Plus A successor to ARCnet that supports communication up to 20Mbps.

ARPA See Advanced Research Projects Agency.

ASCII See American Standard Code for Information Interchange.

ASCII character set A 7-bit character set widely used to represent letters and symbols found on a standard U.S. keyboard. The ASCII character set is identical to the first 128 characters in the ANSI character set.

asynchronous communication A communication method where data is sent as a serial stream of information with start and stop bits indicating where the data begins and ends.

Asynchronous Transfer Mode (ATM) A packet-switched WAN technology that breaks up data into 53-byte cells. ATM can reach speeds up to 622Mbps using current technology.

ATM See Asynchronous Transfer Mode.

Attached Resource Computer Network (ARCnet) Created by Datapoint Corporation in 1977, a very flexible and inexpensive network architecture. ARCnet uses a token-passing scheme to connect up to 255 nodes over twisted-pair, coaxial, or fiber-optic cable. ARCnet is limited to speeds of 2.5Mbps.

Attachment Unit Interface (AUI) The connector used with 10Base5 Ethernet (Thicknet). It is often found as one of the ports on the back of a network interface card (NIC) and is also referred to as a DIX connector.

attenuation The degeneration of a signal over distance on a network cable. As an electrical signal travels farther along a cable, part of the signal is absorbed by the network media, eventually rendering the signal unreadable by receiving network nodes. Attenuation is measured in decibels.

auditing The process of monitoring user activity on a network to track unauthorized or unintentional network usage. Auditing can be enabled to track such items as logon attempts, directory creation, file modification, and password changes. Auditing normally involves the creation of log files that track these system events.

AUI See Attachment Unit Interface.

AWG See American Wire Gauge.

B

back end In client/server applications, the software component running on the server that communicates with the front end or client software.

backbone The main cable segment to which other network devices are connected. While in 10Base5 networks, transceivers are connected directly to a Thicknet backbone; in other networks, the term is used to refer to whatever cable is connecting different network segments together.

backup A duplicate copy of an item made for the purpose of protecting the item. The term is also used to refer to the process of duplicating data. Backing up data is also referred to as archiving.

backup domain controller (BDC) Within a Windows NT Server domain, maintains a duplicate read-only copy of the domain security database and provides security validation in the event of the failure of the primary domain controller (PDC). See primary domain controller.

bad-sector remapping See sector-sparing.

bandwidth In network media, refers to the number of bits that can be sent across the cable at any given time.

barrel connector A hardware device used to connect two coaxial cables.

base input/output (I/O) port The address the processor uses when communicating with the motherboard. Like the IRQ, the base I/O port of a device must be unique.

base memory address Also referred to as the upper memory address (UMA), the starting address in the buffer area of the computer's memory (RAM) for the network interface card.

baseband transmission Uses digital technology where the 1's and 0's of the data bits are defined as discrete changes in the flow of electricity or light. The entire communication channel is used to transmit a single data signal.

baud rate A measurement of modem speed named for a French scientist named Baudot who developed an encoding scheme for the French telegraph system in 1877. Often confused with bps (bits per second), the baud rate actually refers to the number of state transitions (from 0 to 1 and 1 to 0) that occur within a single second. Newer compression technologies allow more than 1 bit to be transmitted within a single state transition, so the two measurements are no longer equivalent. A modem transmitting at 9,600 bps might in fact transmit at 2,400 baud.

BDC See backup domain controller.

beaconing The process that allows networks to self-repair network problems. The stations on the network notify the other stations on the ring when they are not receiving transmissions. Used primarily in Token-Ring and FDDI networks. See Token Ring and FDDI.

binding The process that links a protocol driver and a network adapter driver.

bit Short for BInary digiT, the smallest unit of data a computer can store. Bits are expressed as 1 or 0.

BNC (British Navel Connector) A connector used for coaxial cable.

bottleneck A network device that causes network traffic to be significantly slowed.

bps A measurement within communications of the number of bits per second transmitted.

bridge A device used to combine different segments of a network into one large network. Bridges can work as repeaters to extend a network and connect network segments, and they can also filter network traffic to reduce congestion. The bridge connects networks at the Data Link Layer of the OSI Model.

bridging table A comprehensive list of hardware (MAC) addresses for the network. This table is used by a bridge to determine which packets should be delivered to which ports.

broadband transmission Uses analog communication to divide the network cable into a series of channels. Each channel has its own frequency, and all devices listening at that frequency can obtain the data.

broadcast infrared Disperses the infrared signal so that multiple units can receive the transmission. See also infrared.

broadcast packets Data packets that are sent to all the computers on the network.

broadcast storm Occurs when a network device (network interface card or network application) malfunctions and starts to deluge the network with broadcast packets. Routers can be used to limit the effects of broadcast storms.

brouters Hybrid devices that combine features of both bridges and routers and are only found in networks using multiple protocols. A brouter routes routable protocols and bridges nonroutable protocols.

browse To look through a list on a computer system. Lists include directories, files, domains, or computers.

browser On the Internet, a software program used to view documents on the World Wide Web. Also used within the world of Microsoft networks to refer to the computer maintaining a list of NetBIOS names currently in use on the network.

buffer A temporary holding place reserved in memory, where data is held while in transit to or from a storage device or another location in memory.

buffering The process of using buffers, particularly to or from I/O devices such as disk drives and serial ports.

bus A network topology where all the computers are connected together in a line. Messages are passed between the computers along a single backbone with a terminator located at the end to stop the network signal. The term can also refer to the data bus used within a computer to communicate between the CPU and hardware components.

bus mastering Similar to direct memory access (DMA), a technique where your network interface card (NIC) takes control of the computer's data bus and transfers data directly into the system memory without involving the microprocessor. See Direct Memory Access (DMA).

byte 8 bits.

C

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Similar to CSMA/CD, computers will first check the network media to see if it is in use. Before transmitting the data, the computer will send out a signal indicating that it is about to transmit. After the signal has gone out, then the computer will actually transmit. Used in AppleTalk networks with LocalTalk media.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) The basis for the Ethernet network architecture, where multiple computers have access to the network media. The computers will check the network media before transmitting to see if it is being used. If two or more computers transmit at the same time, a collision is detected and each computer will wait a random period of time before retransmission.

CCITT (Comité Consultatif Internationale de Télégraphie et Téléphonie) The Geneva-based international organization that specifies communications standards used throughout the world, also referred to as the International Telegraph and Telephone Consultative Committee. The CCITT is part of the International Telecommunications Union (ITU), a United Nations body. Many CCITT standards are now being referred to as ITU standards.

cell The 53-byte data packets used by ATM.

cell-switching The process in which data packets are broken into very small, fixed-length cells that are transmitted across the network.

central office (CO) The office of a local telephone company to which all local phone lines within a region are connected. WAN connections typically involve a link (the "local loop") from your office to the nearest CO where connections are then made to long-distance carriers. See local loop.

central processing unit (CPU) The computational and control unit of a computer; the device that interprets and executes instructions. The CPU or microprocessor, in the case of a microcomputer, has the ability to fetch, decode, and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus. The CPU is the chip that functions as the "brain" of a computer.

Channel Service Unit/Data Service Unit (CSU/DSU) A hardware device used to connect a computer network to a digital line used in WAN communication.

character A letter, number, punctuation mark, or a control code. Usually expressed in either the ANSI or ASCII character set.

checkpoints Bits of data placed in the data stream at the Session Layer of the OSI model to facilitate recovery from network transmission problems. If a network failure occurs, only data transmitted since the last checkpoint will need to be retransmitted.

circuit In network communications, a communication path between two network endpoints.

circuit-switched network A switched network in which a communication channel is established between two endpoints for the duration of a communication session. The telephone system is an example of a circuit-switched network.

cladding A layer of glass surrounding the central fiber of glass inside a fiber-optic cable. The purpose of the cladding is to reflect the light that is being transmitted down the fiber, back into the central fiber. This prevents the light from traveling in all directions.

client A computer that accesses shared network resources provided by another computer, called a server. See also server.

client-access licenses Licenses for network applications specifying how many users can use the application.

client/server architecture A network architecture that divides processing between client software located usually on desktop PCs and server software located on servers. The client programs handle user interaction and make requests for data. Server programs process data and fulfill requests from clients.

client software Software that allows users to access and use network resources such as file servers and printers.

coaxial cable Also referred to as coax, consists of an inner wire core that transmits the data and an outer layer of electrically conductive shielding to reduce interference. Within Ethernet networks, Thinnet and Thicknet are common coaxial cables.

collision A situation where two or more network devices transmit simultaneously.

communications protocol The rules that govern a conversation between two computers that are communicating via an asynchronous connection.

computer name A unique name that identifies a particular computer on the network. Microsoft networking uses NetBIOS names, which can have up to 15 characters and cannot contain spaces.

concentrators A generic term for a device that provides a central connection point for the connection of terminal, computer, or communications devices. Also, a specific term used to refer to an FDDI hub.

contention The situation when multiple devices compete for the use of the network media. Contention-based access methods, such as CSMA/CD, provide rules for governing contention and limiting collisions. See CSMA/CD.

controller See domain controller.

CPU See central processing unit.

CRC See Cyclical Redundancy Check.

crosstalk Occurs when two wires are placed next to each other inside a cable. The noise from each line can interfere with the signal in the other line.

CSMA/CA See Carrier-Sense Multiple Access with Collision Avoidance.

CSMA/CD See Carrier-Sense Multiple Access with Collision Detection.

CSU/DSU See Channel Service Unit/Data Service Unit.

Cyclical Redundancy Check (CRC) A number produced by a mathematical calculation and added at the end of a data packet before transmission. Upon receipt, the CRC is recalculated and compared against the transmitted number to ensure that the data was not corrupted during transmission.

D

DARPA See Defense Advanced Research Projects Agency.

DAS See Dual Attachment Stations.

data frame The structured packets into which data is placed by the Data Link Layer.

database access language A language such as SQL used to extract information from a database. See Structured Query Language (SQL).

Database Management Systems (DBMS) A sophisticated software system that manages communications between users and the database program.

database servers Servers on a network dedicated to the task of fulfilling database requests.

datagram A packet of information and delivery data that is routed on a network.

Data Link Layer The layer of the OSI Reference Model that is responsible for packaging data into frames and providing an error-free link between two computers. The Data Link Layer was further subdivided by the IEEE 802 Project into the Logical Link Control and Media Access Control sublayers.

DBMS See Database Management Systems.

DECnet A protocol suite developed by Digital Equipment Corporation.

dedicated server A computer that is used only as a server and not as a client workstation.

Defense Advanced Research Projects Agency (DARPA) An agency of the U.S. Department of Defense that sponsored the development of the protocols which became the TCP/IP suite. DARPA was previously known as ARPA, the Advanced Research Projects Agency, when ARPAnet was built.

demarcation point The place at your home or office building to which your local telephone company brings in all phone lines. The telephone company is responsible for all line and equipment maintenance from the local phone network up to the demarcation point. As the customer, you are responsible for all interior wiring from the demarcation point to your telephones or telephone system. Also referred to as the demarc.

device A generic term for a computer component, such as a printer, serial port, or disk drive. A device frequently requires its own controlling software called a device driver.

device driver A piece of software that translates requests from one form into another. Most commonly, drivers are used to provide a device-independent way to access hardware.

DHCP See Dynamic Host Configuration Protocol.

Dial-Up Networking (DUN) Formerly known as remote access service (RAS), provides remote access to networks. DUN allows a remote user to access his network. Once connected, it is as if the remote computer is logically on the network; the user can do anything that he could do when physically connected to the network.

digital A signal with only two states, such as 1's and 0's. Computers and most electronic networking devices use digital communication. For an opposite, see analog.

digital volt meter (DVM) A basic electronic tool that measures the amount of voltage passing through a given electrical circuit. In network communications, a DVM can be used to test continuity to determine if a cable has any breaks.

DIP switch Short for Dual Inline Package switch. Used to configure hardware options, especially on adapter cards.

Direct Memory Access (DMA) A technique used by hardware adapters to store and retrieve information from the computer's RAM memory without involving the computer's CPU.

direct-sequence modulation A form of spread-spectrum transmission that breaks data into chips and then transmits that data on several frequencies.

Directory Services A means of locating users on a network or messaging system. Some e-mail examples include Microsoft's Personal Address Book and Global Address List. Also, X.500 is an international standard for directory services.

disk duplexing A data protection technique similar to disk mirroring, but involving the use of multiple disk drive controller cards to provide extra protection from failures.

disk mirroring A data protection technique where data is simultaneously written in the identical manner on multiple disk drives. If one drive fails, the data will still be available on the second drive. Disk mirroring usually uses two or more disk drives with a single disk drive controller card.

distance-vector algorithm A method used in building routing tables where a cost is calculated for each route based on the number of routers (or hops) in between two networks.

DIX connector Another name for the AUI connector. The name is derived from the creators of the connector: Digital Equipment Corporation, Intel, and Xerox. See AUI.

DMA See Direct Memory Access.

DMA channel A channel for DMA transfers, those that occur between a device and memory directly, without involving the CPU.

DNS See Domain Name Service.

DNS name servers The servers that hold the DNS name database, and supply the IP address that matches a DNS name in response to a request from a DNS client. See also Domain Name Service.

domain For DNS, a group of workstations and servers that share a single group name. For Microsoft networking, a collection of computers that share a security context and account database stored on a Windows NT Server domain controller. Each domain has a unique name. See also Domain Name Service.

domain controller The Windows NT Server computer that authenticates domain logons and maintains a copy of the security database for the domain. See primary domain controller and backup domain controller.

Domain Name Service (DNS) A static, hierarchical name service for TCP/IP hosts. Do not confuse DNS domains with Windows NT domains.

drive designators The disk drive letters used by a client redirector to make network resources appear as if they are local.

driver A small piece of software that is installed into the operating system to allow it to use a specific device—for example, the printer or network interface card (NIC).

dual attachment concentrators In FDDI, these are connected to both rings and have ports allowing the connection of workstations. Similar to hubs in other architectures.

Dual Attachment Stations (DAS) FDDI network interface cards that are attached to both rings and are intended primarily for servers, concentrators, and other devices that need the reliability afforded by the dual-ring structure.

DVM See Digital Volt Meter.

Dynamic Host Configuration Protocol (DHCP) A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

dynamic routers Choose the best route for the data packet to travel. In order to calculate which route is better, the dynamic routers use two methods: distance-vector algorithm and link-state algorithm.

E

EISA See Extended Industry Standard Architecture.

electromagnetic frequency The number of wave cycles per second, measured primarily in terms of hertz (Hz).

electromagnetic interference (EMI) A type of signal that interferes with the correct transmission of signals through a network medium. For instance, electrical motors placed in close proximity to network cables could generate enough EMI to interfere with the network signal passing through the cables.

electromagnetic spectrum The range of the transmission of energy waves from electrical power and telephones at the low end to X-rays and gamma rays at the high end.

electronic mail (e-mail) An electronic message sent from one user to another.

electronic messaging system (EMS) A system that allows users or applications to correspond using electronic mail.

e-mail See electronic mail.

e-mail client In an e-mail system, the program responsible for all the user interaction, such as reading and composing messages. Also called a User Agent (UA).

EMI See electromagnetic interference.

encryption The process of encoding messages so they cannot be read during transmission.

enterprise (or enterprise-wide) network See wide area network.

Ethernet A LAN network architecture originally developed by Xerox in 1976 and later standardized as IEEE 802.3. Designed to use a bus architecture and the CSMA/CD access method, and to transmit data at 10Mbps. Uses coaxial, twisted-pair, or fiber-optic cable.

Ethernet 802.2 The default Ethernet frame type used in Novell NetWare 4.x networks.

Ethernet 802.3 Also referred to as raw Ethernet, the Ethernet frame type used primarily in Novell NetWare 2.x and 3.x networks.

Ethernet SNAP (SubNetwork Address Protocol) The Ethernet frame type used in AppleTalk Phase II networks.

Ethernet II Ethernet frame type used in TCP/IP networks and networks using multiple network protocols.

EtherTalk Allows a network to use AppleTalk network protocols over 10Mbps IEEE 802.3 Ethernet network.

ev See hertz volt.

Extended Industry Standard Architecture (EISA) An enhancement to the bus architecture used on the IBM PC/AT, which allows the use of 32-bit devices in the same type of expansion slot used by an ISA adapter card. EISA slots and adapters were common in server computers, but have been mostly replaced with PCI slots.

F

fault tolerance A generic computing term for the condition of being able to provide some protection against failure. The fault tolerance of a network is the degree of network problems that can occur before the network fails.

FDDI See Fiber Distributed Data Interface.

Fiber Distributed Data Interface (FDDI) Uses fiber-optic cable and token-passing to create a very fast and reliable network operating at speeds up to 100Mbps. FDDI networks are implemented as a true physical ring.

fiber-optic cable Cable in which the data is transmitted in the form of light rather than electrical signals. Fiber-optic cables are not susceptible to electromagnetic interference which degrades copper wires.

file A collection of information stored on a disk, and accessible using a name.

file sharing The ability of a network computer to share files or directories on its local disks with remote computers. Windows 95 and Windows NT allow you to share your files if the File and Print Sharing services are enabled on your computer.

file system In an operating system, the overall structure in which files are named, stored, and organized.

file transfer protocol (FTP) The standard method of transferring files using TCP/IP. FTP allows you to transfer files between dissimilar computers, with preservation of binary data and optional translation of text file formats.

firewall A security barrier constructed of hardware and software to keep intruders out of a network.

folder In Windows Explorer, a container object—that is, an object that can contain other objects. Examples include disk folders, the Fonts folder, and the Printers folder. A replacement for the term directory.

frame See data frame.

frame relay A packet-switching technology that uses variable-length packets and establishes permanent virtual circuits between endpoints. One reason frame relay networks are popular is that customers can specify the amount of bandwidth they want to use.

frequency-hopping A type of spread-spectrum transmission that switches data between multiple frequencies. Both the transmitter and the receiver are synchronized to use the same predetermined frequencies and time slots.

FTP See file transfer protocol.

G

gateway A computer connected to multiple networks and capable of moving data between networks using different transport protocols. Unlike routers and brouters, gateways can actually change the format of the data itself. Gateways function at the Application and other upper layers of the OSI Model.

Gbps Gigabits per second. Essentially one million bits per second.

geosynchronous satellite A satellite located in a fixed location above one location on the ground.

GHz A frequency measurement representing one billion bits per second.

gigabyte Roughly one billion bytes.

Gopher A distributed information system on the Internet developed by the University of Minnesota. Information is presented as a series of menus.

graphical user interface (GUI) A computer system design in which the user interacts with the system using graphical symbols, tools, and events, rather than text-based displays and commands such as the normal Windows user interface.

group Within a network operating system, user accounts can be placed into group accounts, and permissions can be given to the entire group.

groupware applications Also referred to as workgroup applications, similar to e-mail systems but provide added functionality to enable a group of people to work better together. Groupware systems include Microsoft Exchange, Lotus Notes, and Novell Groupwise, which provide both e-mail and workgroup functions.

GUI See graphical user interface.

H

hertz (Hz) The unit of frequency measurement equal to one cycle per second.

hertz volt (ev) The unit of measurement used when electromagnetic frequencies enter the range of light.

hop When calculating the routing table and determining the best path between two endpoints, each router in the path counts as one hop.

host Another name for any server that is attached to an internetwork.

host ID The portion of the IP address that identifies a computer within a particular network ID.

host name The name of an Internet host. It may or may not be the same as the computer name. In order for a client to access resources by host name, it must appear in the client's HOSTS file, or be resolvable by a DNS server.

host table The HOSTS and LMHOSTS files, which contain mappings of known IP addresses mapped to host names.

HOSTS file A local text file in the same format as the 4.3 Berkeley Software Distribution (BSD) UNIX /etc/hosts file. This file maps host names to IP addresses. In Windows 95, this file is stored in the \WINDOWS directory.

hot-fixing See sector-sparing.

HTML See HyperText Markup Language.

hub A connectivity device used in a star network to provide a central connection point for all cable segments. An active hub, sometimes referred to as a multiport repeater, requires electrical power and regenerates the signal from each cable segment. A passive hub requires no power and merely serves as a central location to organize wiring. A hub, like a repeater, operates at the Physical Layer of the OSI Model.

HyperText Markup Language (HTML) A text file format used to create pages for use in the World Wide Web.

Hz See hertz.

I

ICMP See Internet control message protocol.

IEEE See Institute of Electrical and Electronic Engineers.

IEEE 802 Specifications which define the way in which data is actually placed on the physical network media by network interface cards. The IEEE 802 specification divides the OSI Data Link Layer into two sublayers: Logical Link Control and Media Access Control.

IETF See Internet Engineering Task Force.

IMAP4 See Internet Mail Access Protocol version 4.

impedance The resistance of a wire to the transmission of an electrical signal, measured in ohms.

Industry Standard Architecture (ISA) The designation for the data bus and expansion slots used in the original IBM PC/XT. ISA expansion slots will accommodate an 8-bit or 16-bit card.

infrared (IR) In the electromagnetic spectrum, infrared frequencies occupy the range from 100Ghz through 1,000 terahertz (THz), just below the range of visible light. Infrared communication technology takes two forms: point-to-point and broadcast.

infrared networks Networks that use infrared signals instead of physical cables to connect the computers on a network. Infrared networks are generally limited to line of sight, where the network adapter on the computer must be able to "see" its companion network port.

Institute of Electrical and Electronic Engineers (IEEE) An organization that issues standards for electrical and electronic devices.

Integrated Services Digital Network (ISDN) A digital communications method that permits connections of up to 128Kbps, using two 64Kbps channels. ISDN is designed as a replacement for the traditional telephone system and requires the installation of a digital line.

International Organization for Standardization (ISO) The organization that produces many of the world's standards. Open Systems Interconnect (OSI) is only one of many areas standardized by the ISO.

International Telecommunications Union (ITU) A body of the United Nations that develops standards for global telecommunications. The CCITT is a committee of the ITU. See CCITT.

Internet The worldwide interconnected WAN, based on the TCP/IP protocol suite.

Internet control message protocol (ICMP) A required protocol in the TCP/IP protocol suite. It allows two nodes on an IP network to share IP status and error information. ICMP is used by the ping utility.

Internet Engineering Task Force (IETF) A consortium that introduces procedures for new technology on the Internet. IETF specifications are released in documents called Requests for Comments (RFCs).

Internet Mail Access Protocol version 4 (IMAP4) An Internet protocol for retrieving mail from a mail server. Designed as the successor to POP3.

Internet protocol (IP) The Network Layer protocol of TCP/IP responsible for addressing and sending TCP packets over the network.

internetwork Two or more networks connected together in such a manner that data can be exchanged between networks while both (or all) networks continue to function independently.

interprocess communications (IPC) A set of mechanisms used by applications to communicate and share data.

interrupt An event that disrupts normal processing by the CPU, and results in the transfer of control to an interrupt handler. Both hardware devices and software can issue interrupts; software executes an INT instruction, while hardware devices signal the CPU by using one of the interrupt request (IRQ) lines to the processor.

interrupt request lines (IRQ) Hardware lines on the CPU that devices use to send signals to cause an interrupt. Normally, only one device is attached to any particular IRQ line.

I/O address One of the critical resources used in configuring devices. I/O addresses are used to communicate with devices. Also known as a port.

I/O bus The electrical connection between the CPU and the I/O devices. There are several types of I/O buses: ISA, EISA, SCSI, VLB, and PCI.

I/O device Any device in or attached to a computer that is designed to receive information from, or provide information to, the computer. For example, a printer is an output-only device, while a mouse is an input-only device. Other devices, such as modems, are both input and output devices, transferring data in both directions. Windows 95 must have a device driver installed in order to be able to use an I/O device.

IP See Internet protocol.

IP address Used to identify a node on a TCP/IP network and to specify routing information on an internetwork. Each node on the internetwork must be assigned a unique 32-bit IP address, which is made up of the network ID plus a unique host ID assigned by the network administrator. The subnet mask is used to separate an IP address into the host ID and network ID. In Microsoft networks, you can either assign an IP address manually or automatically using DHCP.

IP router A system connected to multiple physical TCP/IP networks that can route or deliver IP packets between the networks.

IPC See interprocess communications.

IPX/SPX Internetworking Packet eXchange/Sequenced Packet eXchange. Transport protocols used in Novell NetWare networks.

IR See infrared.

IRQ See interrupt request lines.

ISA See Industry Standard Architecture.

ISDN See Integrated Services Digital Network.

ISO See International Organization for Standardization.

ITU See International Telecommunications Union.

J

jumper A small hardware connector that connects two pins together and completes a circuit.

K

K Standard abbreviation for kilobyte; equals 1,024 bytes.

Kbps Kilobits per second; 1Kbps equals 1,024 bps.

KHz An abbreviation for kilohertz, measuring frequency in terms of thousands of cycles per second.

L

LAN See local area network.

LAT See Local Area Transport.

LDAP See Lightweight Directory Access Protocol.

learning bridge See transparent bridge.

leased line A permanently open communication circuit, typically a telephone line, that connects two endpoints forming a private network. Lines are usually leased from local telephone and long-distance carriers.

Lightweight Directory Access Protocol (LDAP) An emerging Internet standard for providing directory services for electronic messaging systems.

link A connection at the LLC Layer that is uniquely defined by the adapter's address and the destination service access point. Also, a connection between two objects, or a reference to an object that is linked to another.

link-state algorithm A method for building routing tables that takes into account factors such as network traffic, connection speed, and assigned costs when calculating the best route for sending data packets.

LLC See logical link control.

LMHOSTS file A local text file that maps IP addresses to the computer names of Windows networking computers. In Windows 95, LMHOSTS is stored in the WINDOWS directory.

local area network (LAN) A computer network confined to a restricted area such as a single building.

Local Area Transport (LAT) A nonroutable protocol used on some networks from Digital Equipment Corporation.

local bus The same high-speed connection used by the CPU to communicate with onboard devices; extended to communicate with peripherals.

local loop A term used in telecommunications to refer to the connection between your network and your phone company's nearest central office. Even when using switched networks, a local connection is required.

local printer A printer that is directly connected to one of the ports on your computer, as opposed to a network printer.

LocalTalk Refers to the cabling system for AppleTalk networks. The ability to use LocalTalk cabling is built into every Macintosh computer. LocalTalk uses STP cable in a bus topology. See AppleTalk.

logical link control (LLC) One of the two sublayers of the Data Link Layer of the OSI Reference Model, as defined by the IEEE 802 standards. This sublayer is responsible for maintaining the link between two computers when they are sending data across the physical network connection.

logical ring A network where the hub is wired so that the signal travels in a ring.

login (or logon) The process by which a user is identified to the computer in a network.

logon script In Microsoft networking, a batch file that runs automatically when a user logs into a Windows NT Server. Novell networking also uses logon scripts, but they are not batch files.

M

M Standard abbreviation for megabyte; 1,024 kilobytes; or 1,048,576 bytes.

MAC See media access control.

MAC address The address for a device as it is identified at the media access control (MAC) layer in the network architecture. MAC addresses (also referred to as hardware addresses) are usually stored in ROM on the network adapter card, and are unique.

mail server A server dedicated to an electronic messaging system.

management information base (MIB) A set of objects used by SNMP to manage devices. MIB objects represent various types of information about a device. See Simple Network Management Protocol.

map The process of designating a disk drive letter to refer to a directory on a file server.

MAPI See Messaging Application Program Interface.

MAU See Multistation Access Unit.

Mbps Megabits per second; 1Mbps equals 1,024Kbps or approximately one million bits per second.

media The mechanism that physically carries a message from computer to computer. Some examples of media include copper cable, fiber-optic (glass) cable, and wireless or radio-based technologies.

media access control (MAC) The lower of the two sublayers of the Data Link Layer in the IEEE 802 network model. This sublayer allows the computers on a network to take turns sending data on the physical network medium. The MAC sublayer is also responsible for ensuring that the data reaches the other computer without any errors.

memory A temporary storage area for information and applications.

message A structure or set of parameters used for communicating information or a request. Every event that happens in the system causes a message to be sent. Messages can be passed between the operating system and an application, different applications, threads within an application, and windows within an application.

Message Handling Service (MHS) The de facto standard for transporting e-mail within Novell NetWare environments. MHS is similar to SMTP and X.400 in that it is not used directly, but rather provides a transport mechanism between e-mail clients and servers.

Message Transfer Agent (MTA) In many electronic mail systems, it is responsible for transporting messages from one user's mailbox to another, or to other MTAs for delivery.

Messaging Application Program Interface (MAPI) An application programming interface that allows a desktop application to work with any underlying electronic mail system.

MHS See Message Handling Service.

MIB See management information base.

Micro Channel Architecture IBM's bus architecture introduced in 1988 that was capable of operating as either a 16- or 32-bit bus.

microwave Electromagnetic waves operating in the GHz frequency range between radio and infrared. Often used for communication between sites where cable is not an option.

MIME See Multipurpose Internet Mail Extension.

modem A communications device that allows two computers to communicate over a telephone line by converting the digital signals from the computers into analog signals to travel over the phone line.

MTA See Message Transfer Agent.

multiplexor (mux) A device that allows several communication channels to share the same physical media. A multiplexor combines the signals at the transmitting end, and a second multiplexor separates the signals on the receiving end.

multiport repeaters Also referred to as active hubs, use electrical power to amplify the data signal, allowing the signal to travel farther and with better clarity along the network.

Multipurpose Internet Mail Extension (MIME) An Internet standard that defines the method in which files are attached to SMTP messages.

Multistation Access Unit (MAU) A Token-Ring hub which is wired as a logical ring.

mux See multiplexor.

N

NADN See nearest active downstream neighbor.

name registration The way a computer registers its unique name with a name server on the network, such as a WINS server.

name resolution The process used on the network to determine the address of a computer by using its name.

named pipe A one-way or two-way pipe used for communications between a server process and one or more client processes. A server process specifies a name when it creates one or more instances of a named pipe. Each instance of the pipe can be connected to a client. Microsoft SQL Server clients use named pipes to communicate with the SQL Server. Also, backup domain controllers use named pipes to communicate with the primary domain controller.

NAUN See nearest active upstream neighbor.

NBF transport protocol NetBEUI frame protocol. A descendant of the NetBEUI protocol, which is a Transport Layer protocol, not the programming interface NetBIOS.

NBT See NetBIOS Over TCP/IP.

NCB See network control block.

NDIS See network device interface specification.

nearest active downstream neighbor (NADN) In Token-Ring networks, the NADN for a specific computer is the next computer in line to receive the token.

nearest active upstream neighbor (NAUN) In Token-Ring networks, the NAUN for a computer is the computer from which it receives the network token.

NetBEUI transport NetBIOS (Network Basic Input/Output System) Extended User Interface. A transport protocol designed by Microsoft and IBM for use on small subnets. It is not routable, but it is fast.

NetBIOS interface A programming interface that allows I/O requests to be sent to and received from a remote computer. It hides networking hardware from applications.

NetBIOS Over TCP/IP (NBT) The networking module that provides the functionality to support NetBIOS name registration and resolution across a TCP/IP network.

network A group of computers and other devices that can interact by means of a shared communications link.

network adapter Another name for a network interface card (NIC).

network analyzer See protocol analyzer.

network applications The applications or programs that run on top of the operating systems and communicate over the network. Some examples of network applications include e-mail programs, File Manager, and the printing systems.

network architecture A term often used to refer to the overall structure of the network, including topology, physical media, and data transmission method. Examples include Ethernet and Token Ring.

network basic input/output system (NetBIOS) A software interface for network communication. See NetBIOS interface.

network control block (NCB) A memory structure used to communicate with the NetBIOS interface.

network device driver Software that coordinates communication between the network adapter card and the computer's hardware and other software, controlling the physical function of the network adapter cards.

network device interface specification (NDIS) In Windows networking, the interface for network adapter drivers. All transport drivers call the NDIS interface to access network adapter cards. An advantage of NDIS is that multiple protocol stacks can use the same network interface card. NDIS was developed by Microsoft and IBM.

network directory See shared directory.

Network File System (NFS) A service for distributed computing systems that provides a distributed file system, eliminating the need for keeping multiple copies of files on separate computers. Usually used in connection with UNIX computers. NFS was developed by Sun Microsystems.

network ID The portion of the IP address that identifies a group of computers and devices located on the same logical network. Separated from the host ID using the subnet mask.

Network Information Service (NIS) A service for distributed computing systems that provides a distributed database system for common configuration files. Used primarily in UNIX systems.

network interface card (NIC) An adapter card that connects a computer to a network.

Network Layer The layer of the OSI Model responsible for addressing a message and routing that message across a network.

network media The physical connection method that runs between the network systems. In most networks, the network media is simply a copper cable; however, network media can also include fiber- optic (glass) cable, and microwave or radio-based media.

network operating system (NOS) The operating system, such as Windows NT Server or Novell NetWare, that is used on network servers. A NOS typically provides file and printer sharing, user administration, and network security.

network protocol The language used in order for computers to be able to communicate. This language is usually described in the cryptic form of TCP/IP, IPX, DLC, and more.

network transport Either a particular layer of the OSI Reference Model between the Network Layer and the Session Layer, or the pro-tocol used between this layer on two different computers on a network.

network-interface printers Printers with built-in network cards, such as Hewlett-Packard laser printers equipped with Jet Direct cards. The advantage of network-interface printers is that they can be located anywhere on the network.

next station identifier (NID) In an ARCnet network, the NID for a specific computer is the numerical ID of the next computer that should receive the token. It is similar to the NADN in Token Ring networks.

NIC See network interface card.

NID See next station identifier.

NIS See Network Information Service.

node A generic term for any device such as a server or workstation that can communicate on a network.

noise Essentially another term for electromagnetic interference. Generally thought of as the random electrical signals which can distort the signal on a network cable.

NOS See network operating system.

O

ODBC See Open Database Connectivity.

ODI See open data-link interface.

ohm The unit of measurement for electrical resistance.

onboard microprocessor A separate microprocessor on the NIC to handle data transfer. This will speed up data throughput by removing the need for the computer's central processor to process the actual data.

Open Database Connectivity An application programming interface by Microsoft that allows Windows application developers to integrate database connections into their applications.

open data-link interface (ODI) Similar to NDIS, allows NIC device drivers to be written without concern for which protocols will be using the NIC. As Novell developed ODI, you will find it widely used within NetWare networks.

open shortest path first (OSPF) An algorithm used in link-state routers. See link-state algorithm.

Open Systems Interconnect (OSI) The networking architecture reference model created by the ISO. The OSI Reference Model breaks down the communication into the following seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical.

operating system (OS) The software that provides an interface between a user or application and the computer hardware. Operating system services usually include memory and resource management, I/O services, and file handling. Examples include Windows 95, Windows NT, and UNIX.

optical fiber See fiber-optic cable.

OS See operating system.

OSI See Open Systems Interconnect.

OSPF See open shortest path first.

P

packet A generic term for a block of data transmitted across a network between two network nodes. The term can also be used more specifically to refer to a transmission unit of fixed maximum size that consists of binary information representing data, addressing information, and error-correction information, created by the Data Link Layer.

packet-switched network A switched network where data is broken into small packets and sent across the network. Each packet may follow a completely different path to the destination according to the best route available.

parity Refers to an error-checking procedure in which the number of 1's must always be the same (either even or odd) for each group of bits transmitted without error.

passive topology When the computers on the network simply listen and receive the signal, they are referred to as passive because they do not amplify or manipulate the signal in any way. An example of a passive topology would be the linear bus or bus topology.

password A security measure used to restrict access to computer systems. A password is a unique string of characters that must be provided before a logon or an access is authorized.

path The location of a file or directory. The path describes the location in relation to either the root directory, or the current directory—for example, C:\Windows\System. Also, a graphic object that represents one or more shapes.

PC Card The specification for credit-card size adapter cards used primarily in laptop computers. Previously called PCMCIA cards.

PCI See Peripheral Component Interconnect.

PDC See primary domain controller.

PDN See public data network.

peer-to-peer networks Networks which allow computers to act as both a client using resources and a server sharing resources. In a peer-to-peer network, there is no centralized control over resources such as files or printers.

peers Computers in a network acting as both a client and a server. These computers are capable of using network resources while simultaneously sharing their own resources with others.

performance monitoring The process of determining the system resources an application uses, such as processor time and memory. Most Microsoft operating systems include performance monitoring tools.

Peripheral Component Interconnect (PCI) The local bus being promoted as the successor to VL. This type of device is used in most Intel Pentium computers and in the Apple PowerPC Macintosh. See VL.

permanent virtual circuit (PVC) A virtual circuit that is established across a packet-switched network for a permanent connection—for instance, between two routers that are always online.

persistent connection A network connection that is restored automatically when the user logs on.

Personal Computer Memory Card International Association (PCMCIA) See PC Card.

Physical Layer The lowest layer of the OSI Model responsible for the actual generation of a signal across the network media.

piercing tap See vampire tap.

pixel Short for picture element, a dot that represents the smallest graphic unit of measurement on a screen. The actual size of a pixel is screen-dependent, and varies according to the size of the screen and the resolution being used. Also known as pel.

platform The hardware and software required for an application to run.

plenum Within an office building, the space between the false ceiling and the office floor above. Often used to circulate air and provide conduits for wiring.

plenum cabling Cables that are more resistant to fire and do not produce as many fumes. Plenum cabling is required by fire safety codes when installing network cabling in false ceilings or other spaces with limited air circulation.

Plug and Play (PnP) A computer industry specification, intended to ease the process of configuring hardware.

Plug and Play BIOS A BIOS with responsibility for configuring Plug and Play cards and system board devices during system power-up, and providing runtime configuration services for system board devices after startup.

point-to-point A generic term for a dedicated connection between any two points on a network. Frequently used to refer to leased lines connecting two networks together.

point-to-point infrared Uses a highly focused narrow beam of energy to connect two sites at high data transmission speeds. See also infrared.

Point to Point Protocol (PPP) The industry standard that is implemented in Dial-Up Networking. PPP is a line protocol used to connect to remote networking services, including Internet Service Providers (ISPs). Prior to the introduction of PPP, another line protocol, SLIP, was used.

polling Within an electronic mail system, the process of constantly checking for mail.

POP3 See Post Office Protocol version 3.

port The socket that you connect the cable for a peripheral device to. See I/O address.

port ID The method TCP and UDP use to specify which application running on the system is sending or receiving the data.

Post Office The message store used by electronic mail systems such as Microsoft Mail to hold the mail messages. It often exists only as a structure of directories on disk, and does not contain any active components.

Post Office Protocol version 3 (POP3) An Internet protocol for the retrieval of electronic mail from a mail server.

PPI See Productivity Point International.

PPP See Point to Point Protocol.

Presentation Layer The layer of the OSI Reference Model which prepares the data to be presented to either the network (if inbound) or the applications (if outbound). This level is responsible for translating, formatting, and encrypting the data as well as the compression of the data when necessary.

primary domain controller (PDC) Within a Windows NT Server network, the PDC is a server that, among other duties, maintains the master list of domain information. There can be only one PDC within a single Windows NT domain.

process The virtual address space, code, data, and other operating system resources—such as files, pipes, and synchronization objects—that make up an executing application. In addition to resources, a process contains at least one thread that executes the process' code.

Productivity Point International (PPI) An international computer training provider offering Microsoft certification courses and testing centers.

propagation delay The delay caused by the time needed to regenerate the data transmission signal as the signal passes through repeaters on the network.

protocol A set of rules and conventions by which two computers pass messages across a network. Protocols are used between instances of a particular layer on each computer. Windows 95 and Windows NT include NetBEUI, TCP/IP, and IPX/SPX-compatible protocols. See also communications protocol.

protocol analyzer A troubleshooting device that monitors network activity and can produce statistics about network performance.

protocol stack A group of protocols, sometimes referred to as protocol suites.

PSTN See Public Switched Telephone Network.

public data network (PDN) A commercial packet-switching service offered by a service provider, typically using X.25 technology.

Public Switched Telephone Network (PSTN) A technical term for the common telephone system.

PVC A term used for a permanent virtual circuit (see permanent virtual circuit) or to refer to the plastic (polyvinyl chloride) outer casing of most network cables.

R

RAID See Redundant Arrays of Inexpensive Disks.

radio network A network that uses radio waves instead of physical cables to connect computers together on a network.

RAM see random-access memory.

RAM buffering As data flows at a high speed from the computer's data bus, the information can be temporarily held in a RAM buffer while awaiting transmission out onto the network media. This process can greatly increase the speed of the network adapter.

random-access memory (RAM) The computer's main memory where programs and data are stored while the program is running. Information stored in RAM is lost when the computer is turned off.

redirector The networking component that intercepts file or print I/O requests and translates them into network requests. The redirector is what allows a client computer to access the network. It operates at the OSI Presentation Layer.

redundant See redundant.

Redundant Arrays of Inexpensive Disks (RAID) A method for providing fault tolerance by using multiple hard disk drives. Broken into five levels (RAID 0 through RAID 5), RAID technologies vary in cost, performance, and protection.

relay towers Towers with mounted repeaters used to extend radio or microwave signals across great distances.

remote access service (RAS) See Dial-Up Networking.

remote administration The process of administrating one computer from another computer across a network.

remote procedure call (RPC) An industry-standard method of interprocess communication across a network. Used by many administration tools.

repeater A hardware device used to extend the transmission distance of a signal by amplifying or regenerating the signal before passing it along. Repeaters operate at the OSI Physical Layer and have no knowledge of the actual data being transmitted.

requestor See redirector.

Requests for Comments (RFCs) The official documents of the Internet Engineering Task Force that specify the details for protocols included in the TCP/IP family.

RFC See Requests for Comments.

ring A network topology that connects all the computers in a single loop. Information is passed along in a continual circle. Each computer acts as a repeater, and token passing is usually used for network access.

RIP See routing information protocol.

routable protocol A protocol such as TCP/IP or IPX/SPX that can be used with a router.

router A connectivity device that connects two or more networks at the OSI Network Layer. A router uses a routing table of network addresses to determine where a data packet should be sent. As routers work at the Network Layer, they can be used to transmit information between different network architectures. While the term router often refers to an actual hardware device, a router can also be a computer with two or more network adapters, each attached to a different subnet.

routing The process of forwarding packets until they reach their destination.

routing information protocol (RIP) A protocol that supports dynamic routing. Used between some routers.

routing table A table used by a router consisting of network addresses.

RPC See remote procedure call.

RPC server The program or computer that processes remote procedure calls from a client.

S

SAP See service access points.

SAS See Single Attachment Stations.

satellite microwave A form of microwave communication which uses the higher frequencies of the low gigahertz range to offer higher transmission rates. Signals will be transmitted between antenna located on the ground and satellites orbiting above the earth.

SCSI See Small Computer System Interface.

sector-sparing A method of providing fault tolerance where the hard disk is checked before data is read or written. If a bad sector is found, the data is moved to a good sector, and the bad sector is marked as unusable. Also referred to as hot-fixing or bad-sector re-mapping.

segment One portion of a network.

sequence number Sequence numbers are used by a receiving node to properly order packets.

Serial Line Internet Protocol (SLIP) The predecessor to PPP, a line protocol supporting TCP/IP over a modem connection. See also Point to Point Protocol.

server A computer or application that provides shared resources to clients across a network. Resources include files and directories, printers, fax modems, and network database services. See also client.

server-based network A network with a centralized control of resources which depends on server computers to provide security and system administration. Server-based networks are sometimes referred to as client/server networks.

server message block (SMB) A block of data that contains a work request from a workstation to a server, or that contains the response from the server to the workstation. SMBs are used for all network communications in a Microsoft network.

server software Software which allows the computer to make network resources available for others to share in addition to performing other administrative functions.

service A process that performs a specific system function and often provides an application programming interface (API) for other processes to call. Windows 95 services include File and Print Sharing and the various backup agents.

service access points (SAP) Series of interface points that allow other computers to communicate with the other layers of the network protocol stack.

Session Layer The layer of the OSI Reference Model that performs name recognition and the functions needed to allow two applications to communicate over the network. This layer handles the opening, using, and closing of a session between two computers.

SFD See Start Frame Delimiter.

share In Microsoft networking, the process of making resources, such as directories and printers, available for network users.

share-level security A network in which there is no central user authentication and control. A resource can be assigned a password at the time at which it is shared to the network. Users need to know the password for each individual shared resource they want to access. Windows 95 and Windows for Workgroups can use share-level security when not part of a Windows NT Server domain.

share name The name that a shared resource is accessed by on the network.

shared directory A directory that has been shared so that network users can connect to it.

shared memory Memory that two or more processes can read from and write to.

shared network directory See shared directory.

shared resource Any device, data, or program that is used by more than one other device or program. Windows 95 can share directories and printers.

sharepoint The network name for a folder, directory, or resource that has been shared by a server or peer computer. The sharepoint can be used to access shared data or services.

shielded twisted-pair (STP) Cable that contains a layer of woven mesh shielding inside the cable that reduces interference and allows a slightly higher transmission speed than UTP. See unshielded twisted-pair.

shielding Foil or woven steel mesh that is wrapped around cable to reduce the interference to an electrical signal in a cable.

SID See station identifier.

Simple Mail Transfer Protocol (SMTP) The Application Layer protocol that supports messaging functions over the Internet. SMTP describes how e-mail servers should send and receive messages.

Simple Network Management Protocol (SNMP) A standard protocol for the management of network components. Windows 95 includes an SNMP agent.

single attachment concentrators An FDDI term equivalent to the hub in other network architectures. May be attached to dual attachment concentrators as a method of allowing more workstations to be connected to the network.

Single Attachment Stations (SAS) FDDI network interface cards that are intended for individual workstations and are attached to a concentrator.

SLIP See Serial Line Internet Protocol.

Small Computer System Interface (SCSI) Pronounced scuzzy, a standard for connecting multiple devices to a computer system. SCSI devices are connected together in a daisy chain, which can have up to seven devices (plus a controller) on it.

SMB See server message block.

SMDS See Switched Multimegabit Data Services.

SMTP See Simple Mail Transfer Protocol.

SNA See Systems Network Architecture.

SNMP See Simple Network Management Protocol.

socket A channel used for incoming and outgoing data defined by the Windows Sockets API. Usually used with TCP/IP.

source-routing bridges Used primarily in IBM Token-Ring environments, rely on the source computer to provide path information within the packet. This type of bridge does not require a lot of processing power because most of the work is being done by the source computer.

SONET See Synchronous Optical Network.

spooler A scheduler for the printing process. It coordinates activity among other components of the print model and schedules all print jobs arriving at the print server.

spread-spectrum Radio communication transmissions that use several frequencies simultaneously. There are two types of spread-spectrum transmissions: direct-sequence modulation and frequency-hopping.

SQL See Structured Query Language.

stand-alone application Applications designed to be operated on a single computer without requiring a network. Examples would be traditional word processors such as Microsoft Word and WordPerfect, or spreadsheets such as Microsoft Excel or Lotus 1-2-3.

stand-alone computer A computer that is not connected to a network.

standby monitor A node on a Token-Ring network that monitors the network status and awaits the signal from the active monitor.

star A network topology where all the computers are connected in a central hub.

Start Frame Delimiter (SFD) A 1-byte field that indicates the beginning of the frame.

static routers Require a network administrator to manually configure the routing table. The router will always use the same route to send the packets even though it may not be the shortest route. If there is no route address, the packet cannot be delivered.

station identifier (SID) The address of an ARCnet computer. Usually configured on the network interface card.

STP See shielded twisted-pair.

Structured Query Language (SQL) A data access language that is used by almost all client/server database applications.

subnet A generic term for a section of a larger network, usually separated by a router or bridge. On the Internet or any TCP/IP network, any lower network that is part of the logical network identified by the network ID.

subnet mask A 32-bit value that is used to distinguish the network ID portion of the IP address from the host ID.

SVC See switched virtual circuit.

Switched Multimegabit Data Services (SMDS) A high-speed packet-switched network server offered in some areas with speeds up to 45Mbps. SMDS is viewed as a competitor to frame relay.

switched virtual circuit (SVC) A virtual circuit that is established across a packet-switched network for a temporary connection between two devices.

synchronous communication A transmission method that relies on exact timing coordination between both the sending and receiving units.

Synchronous Optical Network (SONET) A fiber-optic WAN technology allowing theoretical speeds up to 2.48Gbps and allowing simultaneous transmission of voice, data, and video. Current practical speeds are usually between 155Mbps to 622Mbps.

Systems Network Architecture (SNA) A network architecture developed by IBM and widely used within mainframe networks.

T

T connector A piece of hardware used to connect two coaxial cables.

T1 line The primary type of digital line in use today, providing 24 voice or data channels that can together provide transmission speeds of up to 1.544Mbps. See also T-carrier system.

T-carrier system A telecommunication system developed by Bell Telephone to combine multiple 64Kbps voice or data channels into a single line using multiplexing. A T1 line can support 1.544Mbps, while a T3 line can support 45Mbps.

TCP See Transmission Control Protocol.

TCP/IP See Transmission Control Protocol/Internet Protocol.

TDI See transport driver interface.

TDR See Time-Domain Reflectometer.

Telnet The Application Layer protocol that provides virtual terminal service on TCP/IP networks.

terminal A device used by users to communicate with a host computer, primarily comprised of a monitor (referred to as a CRT, for Cathode Ray Tube) a keyboard, and a network connector (often a RS-232 serial cable).

terminal session Users on a desktop PC can use software to open a terminal session with a mainframe. A window on their PC will behave as if it were a regular terminal.

terminator A hardware device used on a bus network to absorb the signal and to prevent it from bouncing back.

terrestrial microwave Microwave communication system that uses higher frequencies of the low gigahertz range to link two sites. Typically used to link networks together over long distances where using cable is not practical or is cost-prohibitive.

Thicknet The original coaxial cable used in Ethernet networks. Thicknet cable has a thicker core that allows it to transmit data up to 500 meters.

Thinnet A coaxial cable that is easy to install and relatively inexpensive. It transmits data at 10Mbps and has a maximum length of 185 meters.

throughput The amount of data passing through a point on the network in a fixed amount of time. For instance, the throughput of a 10BaseT Ethernet network is theoretically 10Mbps. The term may be used to refer to the overall system or to a specific device such as an NIC or router.

Time-Domain Reflectometer (TDR) A troubleshooting device that sends a pulse down a network cable seeking to find any type of break or problem in the cable.

token A small data frame used in a token-passing network to indicate which computer is allowed to transmit data.

token passing A media access method that eliminates collisions and ensures that every computer gets an equal opportunity to communicate on the network. The token is continually passed around the network, and each computer can only transmit a message when it has the token.

Token Ring A network architecture, developed by IBM in the mid-1980s, that is physically wired using a star topology but is implemented as a logical ring. Token-Ring networks use token passing to ensure that each computer on the network gets a chance to transmit data.

TokenTalk Allows AppleTalk network protocols to be transmitted over a 4- or 16Mbps IEEE 802.5 Token-Ring network.

topology The layout of how computers are physically connected. The three major types of network topologies are the bus, star, and the ring topologies.

transceiver (transmitter/receiver) A device that converts the parallel data stream from the computer's data bus to the serial stream necessary for the network media. Usually included as part of the network interface card, although in 10Base5 networks the transceiver is actually physically connected to the Thicknet backbone.

translation bridge A bridge that allows packets to be translated between network architectures. Primarily used to interconnect a Token Ring and Ethernet network. Also referred to as a transparent source-routing bridge.

Transmission Control Protocol (TCP) A connection-based protocol responsible for breaking data into packets which the IP protocol sends over the network. This protocol provides a reliable, sequenced communication stream for internetwork communication.

Transmission Control Protocol/Internet Protocol (TCP/IP) The primary wide area network used on the worldwide Internet. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic, as well as specifications for utilities.

transparent bridge Used throughout the Ethernet network, these bridges build a bridging table as they receive packets. Also referred to as learning bridges.

transport driver interface (TDI) The interface between the Session Layer and the Network Layer, used by network redirectors and servers to send network-bound requests to network transport drivers.

Transport Layer The level of the OSI Reference Model focused on delivering the data without any errors and in the proper sequence.

transport protocol Defines how data should be presented to the next receiving layer in the networking model and packages the data accordingly. It passes data to the network adapter card driver through the NDIS interface, and to the redirector through the transport driver interface.

twisted-pair Multiple pairs of wire that are twisted around each other inside the cable to prevent crosstalk interference between the wires. Twisted-pair cables come in two variations: unshielded and shielded.

U

UA See User Agent.

UDP See user datagram protocol.

UNC See universal naming convention.

Uniform Resource Locator (URL) An Internet addressing convention that originated with the World Wide Web. The basic format is protocol://servername/pathname.

uninterruptible power supply (UPS) A battery-operated power supply connected to a computer to keep the system running during a power failure.

universal naming convention (UNC) Naming convention, including a server name and share name, used to give a unique name to files on a network. The format is as follows: \\servername\sharename\path\filename.

unshielded twisted-pair (UTP) A type of cable consisting of several pairs of wire, with each pair twisted around each other for a specified number of twists per foot. UTP is the most widespread and easiest cable medium to use. It is also used for telephone systems. UTP is highly susceptible to interference and attenuation, and has a maximum cable length of 100 meters.

UPS See uninterruptible power supply.

UPS service A software component that monitors an uninter-ruptible power supply (UPS) and shuts the computer down gracefully when line power has failed and the UPS battery is running low.

URL See Uniform Resource Locator.

user account Refers to all the information that identifies a user to an operating system, including user name and password, group membership, and rights and permissions.

User Agent (UA) Also called e-mail client, responsible for all the user interaction such as reading and composing messages.

user datagram protocol (UDP) The transport protocol offering a connectionless-mode transport service in the Internet suite of protocols. See transport protocol.

user-level security A network where a central server maintains a listing of all user accounts and provides central authentication of users. On these networks, users normally need only know their one password to logon to the network. After that, they are permitted to use network resources for which they have been granted permission. Windows NT Server networks use user-level security.

user name A unique name identifying a user account in Windows 95. User names must be unique, and cannot be the same as another user name, workgroup, or domain name.

UTP See unshielded twisted-pair.

V

VL Local bus standard for a bus that allows high-speed connections to peripherals, which preceded the PCI specification. Due to limitations in the specification, usually only used to connect video adapters into the system. Also known as VESA bus.

vampire tap Also referred to as a piercing tap, a hardware device used to connect a transceiver to a Thicknet cable. The vampire tap actually pierces the cable insulation and makes direct contact with the central core.

virtual circuit A logical connection between two endpoints across a packet-switched network. The connection can be either temporary or permanent.

volt meter See digital volt meter.

W

WAN See wide area network.

wide area network (WAN) Two or more networks connected usually over a large geographic distance through the use of a long-distance network medium such as the telephone system, microwave towers, or satellites. Also referred to as “enterprise” or “enterprise-wide” networks.

Windows Internet Name Service (WINS) A name resolution service that resolves Windows networking computer names to IP addresses in a routed environment. A WINS server handles name registrations, queries, and releases.

Windows NT The portable, secure, 32-bit, preemptive-multitasking member of the Microsoft Windows operating system family. Windows NT server provides centralized management and security, advanced fault tolerance, and additional connectivity. Windows NT Workstation provides operating system and networking functionality for computers without centralized management.

WINS See Windows Internet Name Service.

wireless bridge A network connection between two LANs using a wireless link, typically in a situation where a cable connection is impossible. Usually implemented with microwave or infrared technology.

workgroup A collection of computers that are grouped for viewing purposes, but which do not share security information. Each workgroup is identified by a unique name. See also domain.

workgroup applications Also referred to as groupware applications, are similar to e-mail systems but provide added functionality to enable a group of people to work better together.

World Wide Web (WWW or Web) The Internet service providing information as a series of pages connected together by hypertext links and incorporating both text and graphics.

X

X.121 The addressing format used by X.25 base networks.

X.25 An international standard for packet-switched networks. Used by some service providers to create public data networks. Because X.25 was created at the time when standard telephone lines were the best communication medium available, it incorporates a high level of error checking and flow control that limits its speed to around 64Kbps.

X.400 An international messaging standard, used in electronic mail systems.

X.500 An international standard for organization information, used as a basis for directories in some electronic mail systems.

Z

zones Groups of computers within an AppleTalk network.



משאבים מומלצים

יכול להיות שספר זה הינו הספר הראשון שלך בנושא תקשורת. כדי לעזור לך בהמשך דרכך בעולם התקשורת אנו מביאים לך פירוט של ספרי התקשורת בהוצאת **הוד-עמי**. עיון ולימוד בעזרת ספרים אלה יעזור לך להיות ולהישאר מקצוען אמיתי בתחום התקשורת.

הוצאת הוד-עמי מציעה מיגוון ספרים בנושא תקשורת מחשבים ברמות שונות של משתמשים. בהמשך, תמצא הסבר על ספרים מומלצים בהוצאת הוד-עמי שיתנו בידך מידע נוסף, מעבר להיקף ספר זה.

- **Windows 2000 Server הכנה למבחן הסמכה**, Microsoft Press, הוצאת הוד-עמי, 1104 עמודים, ספטמבר 2000.

  המדריך הרשמי של Microsoft אשר יקנה לך את הכישורים להם הינך זקוק בעבודתך השוטפת וכדי לעבור את מבחן ההסמכה 70-215# בדרך לקבלת תואר MCSE.

- **המדריך השלם לטכנאי PC - רשתות תקשורת**, מהדורה 2, דורון סיון, הוצאת הוד-עמי, 712 עמודים, ספטמבר 2000.

  הספר המעשי לטכנאי PC בנושא תקשורת המכיל את כל מיגוון הנושאים שטכנאי מחשבים צריך להתמצאות בהם. בליווי דוגמאות מעשיות ומפורטות, תהליכי התקנה ועוד.

- **תקשורת מחשבים - פרוטוקולים וארכיטקטורות רשת**, גולן מוגרבי, הוצאת הוד-עמי, 480 עמודים, פברואר 2000

  כל הפרוטוקולים, כל הארכיטקטורות בתקשורת לפרטי פרטים.

פרקים לדוגמה מכל ספר ומידע מעודכן נוסף תוכל למצוא באתר ההוצאה באינטרנט www.**hod-ami**.co.il.

מידע רישות כללי

באינטרנט תמצא אתרים רבים שעוסקים בהיבטים הכלליים של התקשורת והרישות. אלה הבולטים ביניהם:

http://www.yahoo.com/

http://www.yahoo.com/computers_and_internet/communications_and_networking/

http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Computers/Communications_and_Networking/Hardware/

http://www.yahoo.com/science/engineering/electrical_engineering/telecommunications

http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Software/

חומרה/תווך

למידע אודות תווך פיסי (media) וארכיטקטורות רשת, כדאי שתעיין בדפי מידע של ספקים שונים.

http://www.3com.com/technology/index.html

http://www.eia.org/

http://www.hp.com/rnd/index.htm

http://www.networking.ibm.com/

http://www.intel.com/network/

http://www.ieee.org/

אינטרנט

אם תרצה ללמוד יותר אודות האינטרנט עצמה, תמצא עניין רב באתרים הבאים:

http://www.isoc.org/

http://www.iets.org/

http://www.internic.net/

http://www.thelist.com/

כתבי עת

מקור חשוב למידע בעולם התקשורת המשתנה בקצב מהיר הם כתבי עת אשר יוצאים לאור בתכיפות גבוהה. לפניך כמה מהבולטים יותר:

http://www.commweek.com/

http://www.infoworld.com/

http://www.lanmag.com/

http://www.lantimes.com/

http://www.winntmag.com/

קבוצות דיון באינטרנט

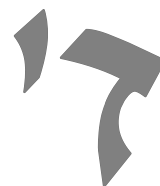
comp.dcom.*

comp.os.ms-windows.networking.*

comp.os.ms-windows.nt.admin.networking

comp.os.ms-windows.programmer.networks

comp.sys.ibm.pc.hardware.networks



התקליטור המצורף

- ✯ **קטלוג HTML** - קטלוג ספרי המחשבים האינטראקטיבי של **הוצאת הוד-עמי**.
לשם קריאת הפרקים לדוגמה יש להתקין את תוכנת Adobe Acrobat Reader אשר מצורפת בתקליטור. הוראות התקנה בהמשך.
הקטלוג מומלץ לצפייה באמצעות Internet Explorer גירסה 5, המצורפת בתקליטור. הוראות התקנה בהמשך.
התקנת שתי התוכנות קלה וניתנת לביצוע באמצעות קישור ישירות מהקטלוג.
- ✯ מספר תוכנות עזר שימושיות.



הערה: אם מנהל התקן כונן התקליטורים המותקן הוא 16 סיביות - ייתכן שתראה רק 8 תווים ראשונים של שם קובץ (במידה שהמקור ארוך יותר).
הסיבה: כונני תקליטורים במהירות x4 עובדים עם מנהל התקן שעבד בסביבת DOS **ו-**Windows 3.11 **ויכול לעבוד גם עם** Windows 95, **למעט היכולת לזהות** קבצים עם שמות ארוכים.
הפתרון: להתקין מנהל התקן 32 סיביות (אם קיים), או לקנות כונן תקליטורים חדש ולוודא שמצורף אליו מנהל התקן 32 סיביות..

קרא את קובץ ONCD שבתקליטור כדי לקבל עוד מידע לגבי התקליטור

התיקיה הרלוונטית לספר זה

בתיקיה **Books\59304** צירפנו קטלוג של חברת טלדור, ישראל. חברת טלדור מתמחה בייצור כבלים לתקשורת מחשבים, מובילה בתכנון ובייצור כבלים להעברת נפחי מידע גבוהים במיוחד. המפעל נמצא בקיבוץ עין דור.

הקטלוג מכיל פרטים של אלפי הכבלים, כולל תמונות, מפרט טכני, תרשימים ופרטים נוספים.

להתקנת הקטלוג יש להפעיל את הקובץ **Setup.exe**

אתם מוזמנים לבקר באתר של חברת טלדור בכתובת:

www.teldor.com

התקנה - Acrobat Reader

יש להתקין תוכנה זו כדי לקרוא ולהדפיס את הפרקים לדוגמה, אליהם ניתן לגשת באמצעות **קטלוג HTML** (שהתקנתו תוסבר בהמשך). התוכנה גם מאפשרת חיפוש בעברית ובאנגלית במסמך המוצג. בנוסף, בעזרת תוכנה זו תוכל לקרוא את המסמכים שההוצאה מפרסמת באתר האינטרנט. התוכנה פועלת במערכות הפעלה **Windows 95 ומעלה!**

1. לחץ על לחצן **התחל** ובחר באפשרות **הפעלה**.
2. בתיבת הטקסט הקלד את הפקודה **X:\Software\Adobe Acrobat\Arme4ENU.exe** (החלף את האות X באות המייצגת את כונן התקליטורים שלך) ולחץ על **אישור**.
3. אשף ההתקנה מתקין את הרכיבים הנדרשים. עליך ללחוץ על **Next**, **Accept** ו-**Next** פעם נוספת כדי לסיים את ההתקנה.
4. בסיום ההתקנה עשויה להופיע על המסך תיבת דו-שיח **התנגשות בין גירסאות** ומייד אחר כך להיעלם. במקומה תופיע על המסך תיבת הודעה של תוכנית ההתקנה. לחץ על **אישור** ובתיבת הדו-שיח **התנגשות בין גירסאות** ששבה להופיע לחץ על **כן**, כדי לשמור את גרסת הקובץ שלך.

קטלוג HTML

הוצאת הוד-עמי גאה לבשר על **קטלוג HTML** העושה שימוש בטכנולוגיות אינטרנט מתקדמות כדי להביא לך את המידע על ספרי המחשבים המקצועיים שלנו בלחיצת עכבר.

מומלץ לצפייה בעזרת Microsoft Internet Explorer מגירסה 5 ומעלה.

בעזרת **קטלוג HTML** תוכל:

- ✯ לעיין במידע על ספרי ההוצאה מתי שתרצה (לחיצה כפולה.... וזהו!).
- ✯ לעבור במהירות ובקלות בין הקטלוג והיישום בו אתה עובד.
- ✯ לעיין במידע על כל ספר וספר.
- ✯ לצפות ואף להדפיס פרק לדוגמה.
- ✯ לגשת במהירות, בגישה אינטואיטיבית, תוך התמקדות מהירה בספר המבוקש.
- ✯ לעיין בקטלוג בקצב אישי שלך.
- ✯ לנווט את דרכך בקטלוג ולחזור ולהתרענן בכל נושא בכל רגע.

הקטלוג מומלץ לצפייה בעזרת Internet Explorer מגירסה 5 ומעלה.

1. הכנס את התקליטור לכונן.
2. לחץ **התחל** ובחר **הפעלה**.
3. בעזרת לחצן עיון סמן את הקובץ **Setup.exe** אשר בתיקיה הראשית של התקליטור המצורף.
4. לחץ **פתח**.
5. לחץ **אישור**.

המחירון המעודכן של ספרי ההוצאה נמצא באתר האינטרנט www.hod-ami.co.il

6. ודא שתקליטור הוד-עמי נמצא בכונן התקליטורים.
7. הפעל את הסמל עם הכיתוב **קטלוג ספרי מחשבים בהוצאת הוד-עמי** שעל שולחן העבודה.



קטלוג ספרי מחשבים בהוצאת הוד-עמי

מה עוד בתקליטור?

הוצאת **הוד-עמי** מפיצה תוכנות אלו כבונוס ללקוחות ההוצאה, ואינה מתיימרת לגבות תשלום עבור התוכניות המצורפות ו/או לתמוך בהם.

אזהרה: השימוש בתקליטור זה הוא על אחריותו הבלעדית של המשתמש. המוצרים המותקנים בתקליטור זה מסופקים באחריות החברות המייצרות אותם. הוצאת הוד-עמי אינה אחראית, בכל צורה שהיא, לאופן ולטיב התוכנות המותקנות.

בכל שאלה לגבי תוכנה הנמצאת בתקליטור, יש לפנות למפתחי התוכנה (כל תוכנה בנפרד) כפי שמצוין בקבצי העזרה של התוכנה המדוברת.

הקבצים הם גרסאות **שיתופיות** (ShareWare) **וחופשיות** (FreeWare).

גרסת ShareWare מאפשרת לך, המשתמש, לבדוק את יעילות התוכנה ואת תאימותה לעבודה אותה אתה מבצע. אם נמצאה התוכנה מתאימה לצרכיך, עליך לשלם למפתחיה תשלום סמלי (לפי הרשום בקבצי העזרה של כל תוכנה ותוכנה בנפרד) כדי לקבל רישיון מלא לשימוש בה. קבלת רישיון לשימוש בתוכנה יפתח בפניך מיגוון אפשרויות שלא עמדו לרשותך בהפעלת גרסת ה-ShareWare.

התקנת תוכנת גלישה לאינטרנט Microsoft Internet Explorer 5

תוכנית ההתקנה מזהה את גרסת מערכת ההפעלה ומתקינה את גרסת הדפדפן הדרושה. מומלץ להסיר גירסה קודמת של Internet Explorer, אם קיימת.

1. הכנס את התקליטור לכונן.
2. לחץ על לחצן **התחל** ובחר באפשרות **הפעלה**.
3. לחץ על לחצן **עיון**.
4. בחר בכונן התקליטורים בתיקיה Software\IE5 ובקובץ בשם SETUP.EXE.
5. לחץ על לחצן **פתח**. לחץ על לחצן **אישור**.
6. פעל לפי ההוראות על המסך.

אזהרה: לפני ביצוע שדרוג מ-Windows 95 ל- Windows 98 בעברית (זו בה התפריטים בעברית ולחצן התחל מימין שורת המשימות), יש להסיר את Internet Explorer 5. לאחר השדרוג ניתן לבצע התקנה מחדש של הגירסה המתאימה.

FontsPekan

קובץ זה יתקין במחשב 2 גופנים בעברית לשימושכם. בסיום ההתקנה יש לבצע את הפעולות הבאות:

1. לחץ על **התחל**, הצבע על **הגדרות**, ובחר ב**לוח הבקרה**.
2. לחץ לחיצה כפולה על הסמל **גופנים**.
3. פתח את תפריט **קובץ** ובחר באפשרות **התקנת גופן חדש**.
4. עבור לתיקיה **C:\FontsPekan**.
5. לחץ על לחצן **בחר הכל** (סה"כ יש בתיקיה 2 גופנים).
6. ודא שתיבת הסימון **העתק גופנים לתיקיית הגופנים** מסומנת.
7. לחץ **אישור**.
8. סגור את חלון התיקיה **Fonts**.
9. סגור את חלון **לוח הבקרה**.

כעת, מוכנים הגופנים לשימוש בכל התוכנות המותקנות במחשב שלך: Word, Excel, PowerPoint וגם בתוכנות גרפיות, כגון Paint Shop Pro ו-PhotoShop.

הגופנים נקראים Tml-JUMP ו-Tml-step ויופיעו בתחתית רשימת שמות הגופנים (בדרך כלל). הרי דוגמה שלהם:

Tml-step

אבגדהוזחטיכךלמםנןסעפףצץקרשת1234567890

Tml-JUMP

אבגדהוזחטיכךלמםנןסעפףצץקרשת1234567890

NETEX

במקום לרשום **http://www.hod-ami.co.il** פשוט רישמו **הוד-עמי** והנה אתם באתר ההוצאה.

במטרה להגיע לאתר מסוים באינטרנט, שכתובתו אינה ידועה, אנו משתמשים בדרך-כלל באחת משתי דרכים: ניחוש של כתובת האתר ו/או פנייה לאינדקס או למנוע חיפוש

שתי הפעולות הן מסורבלות וגוזלות זמן ואנרגיה מיותרים. ניחוש הכתובת מחייב הקלדה של הכתובת המלאה באנגלית בדיוק מושלם, והוא עשוי להיות הליך גוזל זמן, במיוחד כאשר לא מצליחים למצוא את האתר בניסיון ראשון או בכלל.

עם netex לא צריך לנחש כתובות או לגלוש למנועי חיפוש כדי להגיע לאתר מסוים ברשת! פשוט מקלידים את שם האתר בעברית בחלון הכתובת בדפדפן, ומגיעים אליו ישירות.

אפשרויות השימוש במערכת

גלישה ישירה לאתר על-פי שמו או על-פי נתונים הקשורים בו.

מקלידים בחלון הכתובת של הדפדפן שם של אתר או חברה או מילות מפתח הקשורות באתר (בכל סדר שהוא), ומגיעים אליו ישירות.

לדוגמה:

- ✯ מקלידים הוד-עמי או הוצאת הוד-עמי או ספרי מחשבים ומגיעים ישירות לאתר הוצאת הוד-עמי לספרי מחשבים.
- ✯ מקלידים **בנק דיסקונט** - ומגיעים ישירות לאתר של בנק דיסקונט.
- ✯ מקלידים **סלקום** או **052** - ומגיעים ישירות לאתר של חברת סלקום;
- ✯ מקלידים **עכבר העיר** - ומגיעים ישירות לאתר של העכבר;
- ✯ מקלידים **144** - ומגיעים למודיעין 144 של בזק;

התחברות למערכת
הניתוב החדשה של ישראל

כל שעליכם לעשות כדי להתחבר ל-NETEX הוא להתקין תוכנה קלה וחכמה:

1. יש לסגור את כל התוכנות הפתוחות כולל הדפדפנים הפועלים.
2. מתוך סייר Windows הפעילו את הקובץ **netex100.exe** שבתיקיה X:\Software\NetEx.
3. פעלו בהתאם להוראות.

בזמן ההתקנה התוכנה מזהה את הדפדפן/ים שמותקנים במחשב, והיא תפעל עם כולם. מייד אחרי סיום ההתקנה תוכלו להתחיל לגלוש חכם ובעברית.

המערכת שקופה למשתמש, כלומר היא "מתלבשת" על הדפדפן הרגיל ואינה נראית כלל. אין צורך להפעיל אותה או לבצע פעולה כלשהי כדי להשתמש בה: פשוט מקלידים את שם האתר המבוקש בשדה הכתובת של הדפדפן, ומגיעים ישר אליו.

התוכנה אינה מפריעה לעבודה רגילה עם הדפדפן. היא נכנסת לפעולה רק כאשר מקלידים נתון שאינו כתובת אינטרנט רגילה (URL). כאשר תקלידו **www.hod-ami.co.il** תגלשו ישירות לאתר **הוצאת הוד-עמי**, בדיוק כפי שנהגתם לגלוש לפני התקנת התוכנה (ללא מעורבות המערכת). אך אם תרצו, תוכלו להקליד **הוד-עמי** בשדה כתובת ולהגיע במהירות לאותו אתר בדיוק.

תיקיה ראשית SoftWare
(רשימה חלקית ועשויה להשתנות)

הערה: תוכנות להן יש גירסה מיוחדת עבור Windows 2000 יסומנו בתיקיה ששמה מסתיים ב- 2k (למשל, בתיקיה ICQ נמצא קובץ התקנה לתוכנה זו המתאים לכל גירסאות Windows, ובתיקיה ICQ2k נמצא קובץ התקנה עבור מערכת ההפעלה Windows 2000 בלבד).

בדרך כלל לחיצה כפולה על שם הקובץ המפורט ברשימה מפעילה את תוכנית ההתקנה.

שם תוכנה	תיאור
Adobe Acrobat	תוכנה לצפייה בקבצי pdf
Clean System	מחיקת קבצי dll שאין צורך בהם
FontsPekan	גופנים בעברית
ICQ	תוכנה לתקשורת אישית באינטרנט
MIRC	תוכנת הצ'אט הפופולרית ביותר ברשת
NetEx	תוכנה המאפשרת גלישה בעברית
Paint Shop Pro 6	תוכנה ליצירת, עיצוב ועיבוד תמונות
Power Toys	תוכניות שירות עבור Windows 9x
WinAmp	תוכנה להשמעת קבצי MP3 (מוסיקה)
WinZip	תוכנית לפריסה/דחיסה של קבצים
WordView	תוכנית לצפייה בקבצי doc

אינדקס

אינדקס זה הינו באנגלית ולכן כיוון הקריאה שלו הינו משמאל לימין וכן המספור שלו שונה משאר הספר.

Index

Symbols

A

B

C

D

E

F

G

H

I

J - K

L

M

N

O

P

R

S

T

U

V

W

X - Y - Z